Technická univerzita v Liberci

FAKULTA PŘÍRODOVĚDNĚ-HUMANITNÍ A PEDAGOGICKÁ

Katedra: Katedra aplikované informatiky
Studijní program: Informatika
Studijní obor: Informatika se zaměřením na vzdělávání
Anglický jazyk se zaměřením na vzdělávání

OCHRANA OSOBNÍCH ÚDAJŮ NA INTERNETU

PROTECTION OF PERSONAL DATA ON THE INTERNET

Bakalářská práce: 12–FP–KAP–004

Autor:
Ondřej KRAHULEC

Podpis:
.....

Vedoucí práce: RNDr. Pavel Pešat, Ph.D.
Konzultant:

Počet

stran	grafů	obrázků	tabulek	pramenů	příloh
82	3	5	7	93	7

V Liberci dne: 23. 4. 2012

TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta přírodovědně-humanitní a pedagogická
Akademický rok: **2010/2011**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Ondřej KRAHULEC**
Osobní číslo:	**P09001113**
Studijní program:	**B1801 Informatika**
Studijní obory:	**Informatika se zaměřením na vzdělávání**
	Anglický jazyk se zaměřením na vzdělávání
Název tématu:	**Ochrana osobních údajů na Internetu**
Zadávající katedra:	**Katedra aplikované matematiky**

Zásady pro vypracování:

Cíl: Cílem práce je výzkum znalostí žáků 6. a 9. třídy základní školy o ochraně osobních údajů na Internetu a následný návrh doporučení ke zlepšení znalostí o této ochraně včetně návrhu metodických materiálů.

Požadavky:

1. Rešerše problematiky ochrany a zneužití identity a osobních údajů na Internetu ve věkové skupině odpovídající 6. a 9. třídě základní školy.
2. Návrh metodických materiálů pro výuku učiva o ochraně osobních údajů pro věkové kategorie žáků uvedené v bodě 1.
3. Návrh on-line dotazníku pro zjištění znalostí žáků ZŠ ve věkové skupině dle bodu 1 o ochraně osobních údajů.
4. Provedení sběru dat pomocí on-line dotazníku s důrazem na zjištění stavu před výukou relevantního učiva a po ní ve dvou odlišných věkových skupinách. Sběr bude proveden ve školách určených po dohodě s vedoucím práce.
5. Vyhodnocení provedeného výzkumu a úprava metodických materiálů určených pro prezentaci problematiky ochrany osobních údajů.
6. Návrh doporučení pro využití poznatků vyplývajících z výzkumu v praxi.

Rozsah grafických prací:	**dle potřeby**
Rozsah pracovní zprávy:	**cca 45 stran**
Forma zpracování bakalářské práce:	**tištěná/elektronická**

Seznam odborné literatury:

1. **E-bezpečí. Internetový portál. [online]. c2008 [citováno 11. 4. 2011]. ⟨http://www.e-bezpeci.cz/⟩.**
2. **E-nebezpečí. Internetový portál. [online]. c2010 [citováno 11. 4. 2011]. ⟨http://www.e-nebezpeci.cz/⟩.**
3. **KREJČÍ, V. - KOPECKÝ, K. Nebezpečí elektronické komunikace 2 [online]. c2011 [citováno 11. 4. 2011]. ⟨http://www.prvok.upol.cz/index.php/ke-staeni/doc_download/13-nebezpei-elektronicke-komunikace-2-centrum-prvok-2011⟩.**
4. **KREJČÍ, V. - KOPECKÝ, K. Rizika virtuální komunikace [online]. c2010. Net university: Olomouc, 2010. ISBN 978-80-254-7866-O. ⟨http://www.prvok.upol.cz/index.php/ke-staeni/doc_download/13-nebezpei-elektronicke-komunikace-2-centrum-prvok-2011⟩.**
5. **Úřad pro ochranu osobních údajů. Internetový portál. [online]. c2000 [citováno 11. 4. 2011]. ⟨http://www.uoou.cz/⟩.**
6. **HENDL, J. Přehled statistických metod: analýza a metaanalýza dat. 3. přepracované vydání. Praha: Portál, 2009. 695 s. ISBN 978-80-7367-482-3 (váz.).**
7. **ERCES on-line Quarterly Review. [online]. c2004 [citováno 11. 4. 2011]. ⟨http://www.erces.com/journal/Journal.htm⟩. ISSN 1811-9123.**

Vedoucí bakalářské práce:	**RNDr. Pavel Pešat, Ph.D.** Katedra aplikované matematiky
Datum zadání bakalářské práce:	**8. dubna 2011**
Termín odevzdání bakalářské práce:	**30. dubna 2012**

doc. RNDr. Miroslav Brzezina, CSc.
děkan

L.S.

doc. RNDr. Miroslav Koucký, CSc.
vedoucí katedry

V Liberci dne 8. dubna 2011

Čestné prohlášení

Název práce: Ochrana osobních údajů na internetu

Jméno a příjmení autora: Ondřej Krahulec

Osobní číslo: P09001113

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména § 60 – školní dílo.

Prohlašuji, že má bakalářská práce je ve smyslu autorského zákona výhradně mým autorským dílem.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce a konzultantem.

Prohlašuji, že jsem do informačního systému STAG vložil elektronickou verzi mé bakalářské práce, která je identická s tištěnou verzí předkládanou k obhajobě a uvedl jsem všechny systémem požadované informace pravdivě.

V Liberci dne: 23. 4. 2012 .....

Ondřej Krahulec

Poděkování

Rád bych poděkoval svému vedoucímu bakalářské práce panu RNDr. Pavlu Pešatovi, Ph.D. za odborné vedení a cenné rady při tvorbě bakalářské práce i za čas, který mi při konzultacích věnoval.

Poděkovat bych chtěl také své rodině a přítelkyni za podporu, kterou mi poskytovali po celou dobu tvorby práce.

Resumé

Bakalářská práce se zabývá problematikou ochrany osobních údajů na internetu u věkové skupiny odpovídající žákům 6. a 9. tříd. Součástí práce je tvorba metodických materiálů pro vzorovou hodinu, práce dále zkoumá postoje, dovednosti a znalosti této problematiky u žáků 6. a 9. tříd prostřednictvím online dotazníkového šetření a vyvrací jejich výraznější progresivní vývoj. Na základě výsledků výzkumu a praxe jsou formulována doporučení v rovině kurikulární i přímé aplikace v hodinách.

Klíčová slova: osobní údaje, Internet, hesla, sociotechnika, psychopatologické jevy, sociální sítě, Rámcový vzdělávací program, dotazníkové šetření, 6. ročník, 9. ročník, metodické materiály.

Summary

This bachelor thesis explores the issues connected with the protection of personal data on the Internet among sixth and ninth grade students. An important part of the thesis deals with the creation of methodological materials for a model lesson. Furthermore, knowledge, skills and attitudes towards protection of personal data on the Internet among sixth and ninth grade students are measured by means of an online survey. The results of the survey refute progressive development in knowledge, skills and attitudes of the pupils. The thesis also contains recommendations based mainly on the results of the survey. The recommendations are on the level of curriculum as well as application in lessons.

Keywords: Personal data, Internet, Passwords, Social engineering, Pathological Internet use, Social networks, Framework Education Programme, Sixth grade, Ninth grade, Methodical materials

Obsah

Seznam použitých symbolů

p, q, f_i	Relativní četnost
n	Absolutní četnost
n_i	Četnost hodnoty
Q_1	1. kvartil
Q_3	3. kvartil
R	Variační šíře
r_{bb}	Koeficient bodové biseriální korelace
r_p	Pearsonův koeficient korelace
V	Variační koeficient
$\bar{x}, \bar{y}$	Aritmetický průměr
$\tilde{x}$	Medián
$\hat{x}$	Modus
σ	Směrodatná odchylka
$\sum$	Suma

Seznam použitých zkratek

APWG	Anti-Phishing Working Group
COPPA	Children's Online Privacy Protection Act
(D)DoS	(Distributed) Denial of Service
DNS	Domain name systém
FB	Sociální síť Facebook
FFIEC	Federal Financial Institutions Examination Council
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technologies
IKT	Informační a komunikační technologie
IM	Instant Messaging
IP	Internet Protocol
MitM	Man in the Middle
MX	Mail exchanger
RVP ZV	Rámcový vzdělávací program pro základní vzdělávání
RVP	Rámcový vzdělávací program
SMS	Short message service
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
ŠVP	Školní vzdělávací program
TCP	Transmission Control Protocol
TLS	Transport Layer Security Protocol
ÚOOÚ	Úřad pro ochranu osobních údajů
VoIP	Voice over Inernet Protocol
VUT	Vysoké učení technické
XSS	Cross-Site Scripting
ZŠ	Základní škola

Úvod

V souvislosti s rozvojem informačních a komunikačních technologií nabývá na důležitosti i ochrana osobních údajů na internetu. Právě tomuto tématu se práce věnuje a zkoumá jej z nejrůznějších perspektiv.

V teoretické části práce je nejprve prostor věnován definici osobních údajů a jejich právní ochraně a to zejména v kontextu internetu a s přihlédnutím k věku zainteresovaných. V souvislosti s ochranou osobních údajů na internetu je zmíněn důležitý prostor, kde může docházet k nebezpečným praktikám – sociální sítě.

Další část práce je věnována psychopatologickým jevům, které je možné chápat jako pokračování obdobného patologického chování z „reálného světa“ v kyberprostoru. Práce jevy definuje a zabývá se jejich prevalencí mezi dětmi a mládeží, dále na jevy nahlíží s důrazem na problematiku osobních údajů, jejich zneužití či neuvážlivé poskytnutí. Popsány jsou nejprve jevy, kde je zneužití osobní informace nutnou podmínkou pro jejich existenci – sexting (nejčastěji osobní fotografie či video) a též částečně kyberstalking. Dále objasňuje i kybergrooming a doplňkově též některé aspekty kyberšikany a roli osobních údajů v těchto jevech.

Práce dále analyzuje metody sociotechniky, zejména phishingu, sleduje také současné trendy a vývoj této metody. V dalších kapitolách se práce zabývá technickými metodami útoku, které hrají důležitou roli při získávání údajů o uživateli a jeho heslech, jmenovitě se jedná o různé druhy spoofingu, zmíněn je též spyware zejména keyloggery.

V kontrastu s metodami útoku jsou rozebrány i způsoby obrany proti nim počínaje obecnými zásadami přes využití šifrovaných protokolů až k problematice hesel, která je detailněji zkoumána z pohledu uživatelských návyků, možností prolamování hesel a zásady tvorby bezpečného hesla.

Práce v souladu se svým zaměřením na mládež zkoumá problematiku ochrany osobních údajů ve školských dokumentech, dále je provedena analýza výukových materiálů k této problematice, která zahrnuje pestrou škálu od tištěných učebnic přes internetové stránky zabývající se prevencí až k videím a komiksům, které se problematikou zabývají a jsou určené dětem a mládeži. Analýza se neomezuje pouze na materiály české, naopak zkoumá i široké spektrum materiálů zahraničních pocházejících zejména ze Slovenska či anglofonních zemí.

Poslední kapitola teoretické části se zabývá metodou sběru dat, konkrétně realizací online dotazníku a nástroji, které takový sběr umožňují.

V praktické části práce je cílem navrhnout koncepci vyučovací jednotky, která by se zabývala problematikou osobních údajů, vytvořit podrobný plán hodiny a vysvětlit cílové kategorie, kterých je žádoucí dosáhnout společně s prostředky, které k tomu budou využity. Navržená vyučovací jednotka byla prakticky ověřena ve výuce v různých třídách a výsledky vyučování byly ověřeny formou dotazníkového výzkumu.

Dalším cílem praktické části je tvorba dotazníku, který by nám dokázal poskytnout vhled do znalostí, dovedností a postojů žáků 6. a 9. tříd v problematice ochrany osobních údajů na internetu. Kromě popisné statistiky je cílem výzkumu poskytnout i odpověď na dvě hypotézy, první se týká progrese vývoje znalostí, dovedností a postojů v této problematice a to s ohledem na ročník, v kterém žáci jsou. Druhá hypotéza ověřuje, zda vzorové hodiny realizované pomocí plánu měly dopad na výsledky žáků v kontrolní skupině. V rovině popisné jsou výsledky srovnávány v některých ohledech s již prováděnými výzkumy a případné odlišnosti, trendy ve vývoji či zajímavé jevy jsou komentovány a interpretovány.

Na základě reflexe lektorovaných hodin a výsledků výzkumu jsou navrženy změny či doplnění vzorové výukové jednotky a to zejména v rovině konkrétních aktivit. Obecná doporučení jsou potom formulována ve dvou rovinách. První je zaměřena na školské dokumenty a jejich aplikaci v praxi, druhá je příměji cílena na výuku problematiky a to zejména v hodinách ICT a přináší vhled do oblastí, kde je potřeba s žáky pracovat, taktéž přináší možnosti, jak problematiku ochrany osobních údajů do obsahu učiva začlenit.

I. Teoretická část

1 Osobní údaje

V souvislosti s novými informačními a komunikačními technologiemi se objevily případy jejich zneužití v rovině neoprávněného získávání a následného zneužití osobních údajů, např. k identifikaci osoby, podvodnému jednání, při kterém se za danou osobu vydává někdo jiný (krádež identity). Právní rámec osobní údaje chrání a pro nakládání s nimi určuje přísná pravidla.

1.1 Zákony ČR

Dle § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů je osobním údajem *„jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu,“*. [1 § 4, písm. a] Osobními údaji dle zákona tedy nutně musí být rodné číslo či číslo občanského průkazu. Jméno a příjmení společně s datem narození také můžeme považovat za osobní údaje. Pracovní skupina pro informační vzdělávání VUT v Brně mezi osobní údaje dále zařazuje i pohlaví, tituly, bydliště, rodinný stav či místo narození. [2 s. 7–8] Dle zákona takovéto údaje mohou být osobními, pokud je na jejich základě možné subjekt určit – titul v kombinaci s pohlavím nelze považovat za osobní údaje, pokud jsou ovšem doplněny o jméno, příjmení a trvalé bydliště takovéto údaje podléhají ochraně dle zákona č. 101/2000 Sb.

§ 4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů dále rozlišuje i citlivé osobní údaje, takovým údajem je *„osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů,“*. [1 § 4, písm. b]

Osobní údaje mohou být dle výše citovaného zákona shromažďovány a zpracovávány pouze se souhlasem subjektu údajů a to pouze po dobu nezbytně nutnou k danému účelu. [1 § 5–8] [3] Pro citlivé údaje se vztahují pravidla ještě přísnější. [1 § 9–11]

1.2 Problematická interpretace zákona

Problematika definice a klasifikace osobních údajům byla řešena i v roce 2008, kontroverze se týkala IP adres – tyto údaje jsou běžně na internetu zpracovávány a není dbáno žádných zvláštních zásad. Evropská unie tvrdila, že se o osobní údaje jedná, stanovisko vydané ÚOOÚ tvrdilo opak. [4]

Ukazuje se, že i údaje, které zatím nejsou řazeny mezi osobní – velikost bot, oblíbená barva a značka obuvi, koníčky, stravovací návyky, oblíbené stránky atp. mohou ve spojení s jinými daty významným způsobem přispět k identifikaci osoby, a tak de facto hrají roli komponenty osobního údaje. Takovéto údaje, které o sobě běžně uživatelé poskytují, a nejsou nijak chráněny, se velmi brzy začnou stávat (vlastně už začaly) „nepříjemnými údaji, které jsou někde na síti k dispozici“. Nelze s určitostí předvídat, nakolik bude interpretace zákona ve prospěch uživatelů a pomůže jim v budoucnu najít právní ochranu proti vydolování úplně všech údajů, které vydolovat půjdou. Ohledně dataminingu má jisté obavy i Dočekal v již zmiňovaném článku. [4]

1.3 Osobní údaje a děti

Zákon č. 101/2000 Sb., o ochraně osobních údajů ve svém znění nijak neodlišuje děti, pro dětské uživatele sociálních sítí tedy platí stejná pravidla jako pro dospělé (alespoň, co se ochrany jejich osobních údajů týče). V tomto ohledu je praxe v USA odlišná, dětské osobní údaje podléhají přísnějšímu nakládání, dokument, který pravidla upravuje, se nazývá COPPA (Children's Online Privacy Protection Act), je v platnosti od roku 2000 a upravuje sběr osobních údajů u dětí mladších 13 let. Stránky, které jsou cílené na děti a sbírají osobní údaje, musí mít jasně stanovená pravidla pro nakládání s osobními údaji a před sběrem takových údajů o dětských uživatelích musí nejprve získat souhlas jejich zákonných zástupců (takový souhlas má také jisté náležitosti a nestačí pouze souhlas prostřednictvím e-mailu). [5] Tato pravidla jsou mimo jiné i důvodem, proč množství sociálních sítí požaduje, aby jejich uživatelé byli starší 13 let – ušetří jim to množství opatření, která by jinak musely implementovat, aby pravidla COPPA splňovaly, mezi takové sítě patří i Facebook [6] či Twitter [7].

2 Sociální sítě a jejich rizika

2.1 Sociální sítě

Sociální sítě jsou dnes často diskutovaným fenoménem, hovoří se o tom, co uživatelům sítě daly, ale také vzaly. Kopecký a Krejčí je definují takto: „*Sociální sítě je označení pro informační sítě poskytované internetovými portály, které umožňují vytvářet virtuální společenství. Sociální sítě nabízejí prostor pro prezentaci lidí, komunikaci, navazování sociálních vztahů, vzdělávání, komerci (reklama, marketing, sociotechnika) nebo jakoukoli jinou lidskou činnost, kterou lze virtuálně realizovat.“*. [8 s. 22] Na serveru `Bezpečnýinternet.cz` najdeme podstatně méně obsáhlou definici, která ale také zdůrazňuje klíčové prvky: „*Sociální sítě jsou na internetu místem k setkávání lidí, sdílení zážitků, obsahu. Očekává se zde vzájemná interakce.“*. [9] Kopecký ve svém článku o sociálních sítích jako o prostředí pro nebezpečnou virtuální komunikaci definici ještě více zkracuje až na úplnou dřeň: *„sociální sítě jsou virtuální reprezentací lidské společnosti“.* [10]

Analýzou definic můžeme získat klíčové prvky pojmu sociální sítě – lidé, obsah, interakce, online. V zásadě se tyto prvky skutečně přibližují normálnímu lidskému soužití, denně se lidé potkávají a sdělují si zážitky. Nejsou u toho ovšem obvykle nikým sledováni, a pokud ano, jedná se o jednoho člověka a lze jej snadno poznat tak, že je stále na blízku. Zůstávají po rozhovoru se sousedem nějaké záznamy? Nikoliv, pouze v jedincovi paměť. Na sociálních sítích toto neplatí, uživatel je neustále pod drobnohledem každého, komu to dovolí nebo komu to dovolí sociální síť (a mnoho lidí není schopno si soukromí ohlídat, tak, aby nebylo na odiv celému světu). Záznam o činnosti uživatele je trvalý (nebo alespoň dlouhodobý), uložený někde mimo jeho dosah a osobní paměť, Čermák takový záznam nazývá *„nezničitelnou digitální realitou“*, jednoduše je to věc, kterou nelze vzít zpět. [11] Jak je patrné z rozhovoru se zaměstnancem Facebooku pro portál `Therumpus.net`, to, že se něco *smaže* z profilu, neznamená, že by se údaj navždy vytratil z Internetu. [12]

2.2 Oblíbenost sociálních sítí

Pro ilustraci o oblíbenosti sociálních sítí může posloužit údaj o počtu uživatelů sociální sítě Facebook – 845 milionů uživatelů, kteří jsou aktivní každý měsíc, tento údaj pochází z prosince roku 2011. [13] Čísla mohou být do jisté míry zavádějící, nejedná se o unikátní uživatele (takovou statistiku dost dobře ani nelze získat), co je zajímavější než čísla, je trend vývoje. Zatímco v lednu 2009 měl Facebook 150 mil. uživatelů [14] téměř o tři roky později

jich má již zmiňovaných 845 mil. Co se dá dále očekávat? „Pouze“ lineární růst, Facebook bude mít dle odhadů miliardu uživatelů v létě roku 2012. [15]

Stále více lidí se připojuje k sociálním sítím a trend bude pokračovat, jak ale situace vypadá v cílové skupině této práce v naší republice? Kopecký ve své zprávě uvádí, že 90 % respondentů ve věku 11–17 let má svůj účet na sociální síti. [8 s. 23] Toto je údaj, který ani nepotřebuje další komentář.

2.3 Nebezpečí sociálních sítí

Uživatelé sociálních sítí běžně vyplňují své osobní údaje do svých profilů, které jsou často přístupné nejen jejich přátelům (mnoho uživatelů nevyužívá pokročilejšího nastavení svého soukromí nebo jim je to jednoduše jedno). Takto vystavené osobní údaje se mohou stát vhodným materiálem pro další zpracování a zneužití.

Facebook sice implicitně obsah uživatelů mladších 18 let chrání a nastavuje jim vyšší úroveň ochrany soukromí. Šíři údajů, které lze o uživatelích zjistit ukazuje následující příklad. Uživatelka, která má sice ve svém profilu většinu svých informací zakrytou (pro cizí), však odpověděla na stovky anketních otázek a odpovědi jsou viditelné – podle nich lze zjistit téměř vše, věk, zájmy, město bydliště, oblíbený zpěvák, velikost boty, třída kam chodí, škola, oblíbená kosmetika. Takovýto případ není na sociálních sítích zdaleka ojedinělý.

Sociální sítě tedy můžeme nejen na základě udaného příkladu chápat jako bránu či prostředek pro rizikovou komunikaci, ať už se jedná o kyberšikanu, kyberstalking, sexting nebo kybergrooming, o kterých bude řeč v následujících kapitolách.

Údaje vyplněné v profilech mohou být zneužity pro tvorbu falešných identit, nabízení a lepší cílení produktů. Uživatelé se snadno stávají terčem sociálního inženýrství, které ve spojení s údaji získatelnými o uživatelích na sociálních sítích nabírá nový dech a může sloužit k personálnějšímu cílení (dále viz spear phishing). [16 s. 9–11] Uživatelé jsou vlákávání do podvodných skupin či jsou jim rozesílány odkazy na zavirované stránky. Na podobná rizika upozorňuje ve svém článku i Dočekal, který navíc poukazuje na nedokonalé technické zabezpečení Facebooku (ale i jiných sociálních sítí), na Facebooku je možné použít například techniku cross-site scriptingu (XSS) – odkaz sice vede, kam má, ale jako přidanou hodnotu získá uživatel útočníkem podstrčený script, který může například sesbírat jeho osobní údaje. [17]

Sociální sítě nabízejí možnosti, o kterých si předchozí generace mohly nechat zdát, nicméně společně s nimi přináší i velké množství nebezpečí. Uživatel, který se jim chce vyhnout, musí být obezřetný a opatrný v tom, jaké informace o sobě poskytuje.

3 Patopsychologické jevy na internetu

3.1 Sexting

3.1.1 Definice

Kopecký ve své práci definuje sexting jako *„odesílání sexuálně laděných zpráv, fotografií či videozáznamů, jehož cílem je nejčastěji navázání partnerského vztahu mezi odesilatelem a příjemcem nebo jeho zpestření.“*. [8 s. 20] Níže uvedení zahraniční autoři na rozdíl od Kopeckého a Krejčí důvody tohoto počínání nezdůrazňují, spíše popisují samotnou podstatu této rizikové komunikace. Definují sexting jako zasílání sexuálně explicitních materiálů za použití mobilního telefonu [18 s. 23] či zasílání sexuálně explicitních zpráv či svépomocí vytvořených fotografií, zachycujících aktéra nahého či polonahého. [19 s. 542] Zde uvedené zahraniční definice ovšem nepokrývají celou skutečnost, omezují se pouze na jedno médium (telefon) nebo opomíjejí možnost tvorby videí a dalšího šíření. V tomto ohledu se jako nejpřesvědčivější jeví definice Kopeckého a Krejčí.

3.1.2 Sexting mezi mladými

Údaje o výskytu tohoto jevu nejsou v USA jednoznačné. Hojně citovaný a starší „Sex and Tech survey“ uváděl, že svou fotografii či video spadající do definice sextingu odeslalo 20 % mladých ve věku 13–19 let, sexuálně explicitní textovou zprávu potom odeslalo 39 % mladých, takovou zprávu obdrželo 48 % dotázaných. [20 s. 1] Jemnější rozdělení věkových skupin chybí. Oproti tomu novější výzkum z roku 2011 ukázal, že sexuálně laděnou fotografii nebo video, ve kterém se objevili, odeslalo 2,5 % respondentů ve věku 10–17 let, takovou, kde by byla vidět obnažená prsa, pozadí či genitálie odeslalo pouze 1 % dotázaných, takovéto zprávy potom obdrželo větší procento respondentů (7,1 respektive 5,9 %). Dále je z výzkumu patrné, že s rostoucím věkem náchylnost k sextingu vzrůstá. [21 s. 3] Novější výzkum je však diametrálně odlišný od výsledků výzkumu prvního.

Výzkumu sextingu se u nás věnují i Kopecký a Krejčí, ve své studii uvádí, že 10 % respondentů ve věku 11–17 let odeslalo sexuálně laděnou fotografii či video, kde byli nazí či polonazí.

3.1.3 Sexting a ochrana osobních údajů

Obvyklým materiálem sextingových zpráv jsou zejména fotografie a videa, které tedy nechápeme zcela jako osobní údaj dle zákona 101/2000 Sb. V tomto ohledu by tomu odpovídalo i vyjádření ÚOOÚ vydané ke kauze úniku intimních fotografií ze serveru `Líbímseti.cz`

komentované Radimem Hasalíkem. [22] Nicméně je zcela nesporné, že na základě fotografie je často možné jednoznačně identifikovat osobu a navíc může být i nosičem citlivých údajů (etnicita, sexuální život). Nerad bych se pouštěl do výkladu zákona či polemiky na tomto poli, pro potřeby této práce ovšem takovéto materiály budeme považovat za nosiče informací osobního charakteru, které je nutné chránit.

Odeslání takovéhoto materiálu je obzvláště rizikové, jak je vidět z důsledků, které souvisí se zaznamenanými případy (příloha A). Akt odeslání sextingové zprávy může uvolnit lavinu dalších patologických jevů, z nichž některé se odehrávají právě na internetu a jsou popsány dále (kyberstalking, kybergrooming či kyberšikana). U těchto jevů sextingová zpráva s citlivým materiálem, který by jinak měl být subjektem ochrany, působí jako prvotní impuls, případně jako katalyzátor těchto jevů.

3.2 Kyberstalking

3.2.1 Definice kyberstalkingu

Fenomén kyberstalkingu, podobně jako v případě kyberšikany, lze chápat jako přenesení patologického jevu na půdu elektronických médií (mobilní telefony, Internet) a bývá velmi často doprovázen i fyzickou verzí stalkingu. Kyberstalking je dle Jaishankara definován jako použití internetu nebo jiného elektronického média k pronásledování. [23] Kopecký ve své komplexní definici nejprve vysvětluje stalking, aby mohl pomocí něj definovat i kyberstalking: *„Stalking (lov, pronásledování) je termín, který označuje opakované, dlouhodobé, systematické a stupňované obtěžování, které může mít řadu různých forem a různou intenzitu. Pronásledovatel svou oběť například dlouhodobě sleduje, bombarduje SMS zprávami, e-maily, telefonáty či nechtěnými pozornostmi (dárky). Ve spojení s využitím ICT u útočníka hovoříme o termínu kyberstalking (cyber-stalking).“*. [24 s. 3]

3.2.2 Motivace, metody a typy kyberstalkingu

Motivace k takovému jednání může být rozličná, může se jednat o pomstu expartnera, pouhé demonstrování síly, kterou útočník disponuje, či kterou má nad jiným uživatelem, dále sem patří patologická snaha zalíbit se oběti a pokud nejsou city opětovány snaha oběť zničit. Oběťmi stalkingu jsou často celebrity, kterými jsou jejich stalkeři posedlí.

Mezi nejčastější metody, jak se kyberstalking (ale i stalking) projevuje, jsou pozornosti, přehnaná, urgentní a opakovaná vyznání citů, s takovými má osobní zkušenost zhruba třetina dotázaných, tyto mohou být považovány za víceméně neškodné. Naproti tomu například krádež identity či její alterace (tvorba lživých profilů oběti či krádež jejich účtů) je sice méně

častá, osobně ji pocítila 3 % dotázaných, ale v kontextu ochrany osobních údajů je takový jev velmi nebezpečný. [25 s. 79–80]

Kyberstalkery můžeme chápat jako samostatnou kategorii stalkerů, která se neuchyluje k fyzickému kontaktu, v mnohých případech však kyberstalker volně přechází ve stalkera a metody pouze kombinuje k dosažení větší efektivity svého působení. Jaishankar rozlišuje 3 různé druhy kyberstalkingu: [23]

1. E-mail stalking využívá elektronické pošty k jinak klasickým metodám stalkingu od bombardování milostnými vzkazy až po výhružky.
2. Internetový stalking využívá ostatních metod, které Internet nabízí, v současné době takovému chování nahrávají zejména sociální sítě a stále se zdokonalující vyhledávače, což dává staršímu Jaishankarovu modelu další rozměr.
3. Počítačový stalking, vyžaduje již jisté znalosti a jeho klíč tkví v získávání kontroly nad počítačem oběti nebo alespoň sledování její aktivity na počítači např. pomocí keyloggerů.

3.2.3 Ochrana před kyberstalkingem a role osobních údajů

Právní ochrana před nebezpečným sledováním neboli stalkingem je v našem právním systému relativně nová (leden 2010), aby mohl být čin uznán jako stalking musí být činnost stalkera intenzivní, dlouhodobá (4–6 týdnů) a samozřejmě proti vůli oběti. [24 s. 11]

Při rozboru možností jedince vedoucích k účinné obraně proti kyberstalkingu platí stejné zásady jako pro chování na sociálních sítích, dávat všanc co nejmenší množství osobních údajů, které by mohly být zneužity proti jedinci a využívat aktivně nastavení soukromí, které nabízí sociální sítě. Pokud již dojde ke kontaktu a obtěžování kyberstalkerem, je možné využít filtry, blokace e-mailových adres, případně příspěvky nahlásit poskytovateli služeb. V kapitole 3.1 o sextingu byl kyberstalking naznačen jako navazující patologický jev. Intimní fotografie může podnítit další stalkerovo počínání, jak je popsáno v této kapitole, proto je potřeba osobní informace chránit a tak kyberstalkerům pomyslně vytyčit co možná nejmenší hřiště.

Osobní údaje jsou častým cílem kyberstalkerů a právě díky nim dokážou své metody náležitě uplatnit. Kyberstalker bez osobních údajů, potřebných adres či hesel se stává neefektivním. Některé jeho metody bez nich selhávají úplně např. krádeže účtu či tvorba falešné identity, které jsou také druhem kyberšikany a právě v použitých metodách se oba patologické jevy částečně překrývají.

3.3 Kybergrooming

3.3.1 Princip a metody kybergroomingu

„Termín kybergrooming (child grooming, grooming) označuje chování uživatelů internetu (predátorů, kybergroomerů), které má v oběti vyvolat falešnou důvěru a přimět ji k osobní schůzce.“. [26 s. 3] Cílem kybergroomingu je tedy osobní schůzka, kde může útočník podniknout další kroky. Známé jsou případy sexuálního zneužívání podpořeného vydíráním jako v domácím případu Pavla Hovorky [27], dále únos, znásilnění a vražda jako v případu Petera Chapmana. [28]

Pro uskutečnění svého cíle (osobní schůzky) musí groomer nejprve umně využít komunikačních technologií a navodit u oběti pocit bezpečí. Je potřeba, aby si připravil svou falešnou identitu – groomeři se vydávají za někoho jiného, aby byli pro oběti co možná nejatraktivnější. K takovým technikám patří např. tvorba dynamické identity (mění se, jak se to hodí), čirou náhodou má podobné zájmy, vkus atp. jako vytipovaná oběť, svou identitu může dále rozvíjet při kontaktu technikou, která se nazývá mirroring či může přistoupit k maskování své identity jako autority, ze které mohou mít oběti užitek – pořadatel soutěže pro děti atp. [26 s. 5]

Při samotné komunikaci s obětí se snaží útočník oběť manipulovat, aby dosáhl svého cíle, k tomu využívá již zmiňované zrcadlení („ty máš rád hip hop, ten já úplně zbožňuju“), dále úplatků („dobiju ti kredit na mobilu“), může též na oběť naléhat, aby o něm nikomu neříkala („bude to jen naše tajemství“).

V dalším kroku již groomerovi stačí jen dítě vylákat na schůzku a tam se s dítětem sejít. Jak Kopecký poukazuje, útočník se často snaží překlenout věkový rozdíl mezi svými identitami tvrzením, že oběť vyzvedne například rodič. V osobních schůzkách může groomer pokračovat a dále připravovat útok či může využít nátlaku na dítě a vydíráním ho přimět ke splnění svých cílů. [26 s. 7–8]

V celém tomto procesu hrají důležitou roli právě osobní údaje, kvůli jejich zisku útočníkem se dítě stává vydíratelné (zejména pokud poslalo útočníkovi údaje citlivé, např. svou obnaženou fotografii), útočník může svůj útok lépe cílit (mirroring). Dostatečné množství údajů a fotografie také často slouží k prvotnímu výběru oběti, takto si na Facebooku svou oběť vybral i Chapman. [28] Rozbor tohoto případu je možné nalézt v přílohách (příloha B). Kvůli neuváženě umístněným kontaktům může dítě doslova nabídnout komunikační kanál či kanály přes které může groomer začít s manipulací a seznámením, čímž se dostáváme na začátek celého procesu.

3.3.2 Ohrožení kybergroomingem

Studie serveru `Saferinternet.cz` z roku 2009 ukazuje, že téměř dvě třetiny dotázaných ve věku 12–17 let byly požádány o osobní schůzku s někým, koho znali jen online, na takovou schůzku se dostavilo 56 % dětí, v 73 % samy. [29 s. 28–29] Kopecký a Krejčí podávají méně znepokojivý, ale stále alarmující obraz o této problematice ve svém šetření mezi dětmi ve věku 11–17 let. 43 % dětí bylo o schůzku s neznámým požádáno a 23 % na takovou schůzku šlo. Ochotu na takovou schůzku jít, když by byli požádání projevilo 39 % respondentů a ve 20 % případů by nikoho o takové schůzce neinformovali. Z hlediska ochrany osobních údajů je i zajímavé, že fotografii svého obličeje při komunikaci s neznámým na požádání poslalo 38 % dotázaných. [8 s. 19] Na sociálních sítích takové žádosti ani není potřeba, případný groomer má tyto informace volně k dispozici, stačí se pouze zařadit mezi kontakty oběti a někdy ani to ne (v závislosti na nastavení soukromí).

Na základě těchto čísel můžeme konstatovat, že šikovný manipulátor by mohl mít při pokusech oběť vylákat docela slušnou šanci, zejména pokud by své argumenty podpořil například slušně vystylovaným profilem. Otázkou zůstává, kam by se děti nechaly vylákat, což je důležitý faktor toho, zda by byl útok úspěšný.

3.3.3 Kybergrooming a ochrana osobních údajů

Jak již je patrné z výše uvedených podkapitol zabývajících se kybergroomingem, osobní údaje jsou nezbytné pro pokus o kybergrooming. Pokud se predátor nedozví bližší informace o své potenciální oběti, nebude schopen zacílit se na jím vybranou cílovou skupinu jako v případě Petera Chapmana [30] a taktéž nebude ani možné, aby sám sebe stylizoval do vhodné podoby či použil vhodnou techniku (jakými jsou mirroring, profilování nebo fishing) k získání dítěte. [28] Patologický jev kybergroomingu sám o sobě není založen na zneužití osobních údajů – cílem je oběť vylákat. Osobní údaje a další informace osobní povahy o oběti však výrazně zvyšují šance predátora na úspěch, stejně tak ho stimulují k další aktivitě, můžeme je tedy chápat jako katalyzátor kybergroomingu.

3.4 Kyberšikana

3.4.1 Kyberšikana a její spojitost s ochranou osobních údajů

Kyberšikanu definuje Krejčí takto: *„Termínem kyberšikana (cyberbullying) označujeme nebezpečné komunikační jevy realizované prostřednictvím informačních a komunikačních technologií (např. pomocí mobilních telefonů nebo služeb v rámci internetu), jež mají za následek ublížení nebo jiné poškození oběti.“*. [31 s. 3] Definice je velmi široká a zahrnuje mezi

kyberšikanu i kyberstalking, pro tuto práci budeme uvažovat množinu jevů, které zahrnuje výše uvedená definice, ale ne už ty, které by byly zahrnutelné např. do kyberstalkingu. Je sice pravdou, že u těchto jevů je hranice značně neostrá, ale tato práce nechápe kyberstalking jako podmnožinu kyberšikany, což by jinak tato definice implikovala. Kyberšikana by se také dala popsat jako šikana či pokračování šikany jinými prostředky (modernějšími). Její síla tkví v tom, že materiály, které mají za cíl oběti ublížit, obvykle zanechávají dlouhodobou digitální stopu. Útoky jsou snadné a často anonymní, kyberšikana oběť dostihne takřka kdykoliv a kdekoliv, pokud bude používat komunikačních prostředků. Jednoduše nekončí školním dnem.

Pro potřeby této práce se zaměříme pouze na dílčí aspekty, které neopomíjí ani Krejčí a těmi jsou riskantní sdílení a také do jisté míry ztráta zábran ve virtuálním prostoru. [31 s. 7–8] Kompromitující materiál, fotografie či videa totiž můžou poskytnout i samy oběti neuvážlivým sdílením, které již však nejde zvrátit. Osobní údaje, které jednou oběť vystaví, se můžou obrátit proti ní, útočník je může použít ke krádeži identity, může oběť zesměšňovat, kontakty, které oběť poskytne, může využít k zasílání nenávistných vzkazů, spamování atp. V mnohých případech oběť neměla šanci preventivně zasáhnout jako například u happyslappingu (natáčení ponižování na mobilní telefon a následné publikování na síť). [32] Existuje však mnoho případů, kdy si oběť nachystá nevědomky půdu pro kyberšikanu sama ať už sextingovou zprávou (viz příloha A) nebo natočením videa, které se časem stane nechtěným jako v případě Ghyslaina Razy známého spíše jako „star wars kid“ [33].

Pokud se podíváme na frekvenci negativních jevů, které souvisí jak s kyberšikanou, tak s ochranou osobních údajů, zjistíme, že jejich zastoupení zdaleka není zanedbatelné. Obětí prolomení účtu se stalo 33 % respondentů a krádež identity zažilo 8 % dotázaných. [8 s. 13] Minimálně prolomení účtu se dá účinně bránit vhodnými bezpečnostními opatřeními jako je odhlašování se ze školních počítačů, silné přístupové heslo, skryté zadávání hesla či nesdělování hesla ostatním. Krádež identity je do značné míry také ovlivnitelná údaji, které o sobě uživatel sítě poskytuje, může se však stát obětí i bez vlastního zavinění.

4 Sociotechnika

4.1 Princip a typy

Základem sociotechnicky je manipulace na jedné straně a důvěřivost na straně druhé, právě tyto faktory jsou dle Grangerové základem a zároveň definicí sociotechniky. [34] Na základě tohoto zjištění můžeme sociotechniku (též sociální inženýrství) definovat jako snahu útočníka na základě různých technik manipulace vylákat z oběti požadované informace (hesla, osobní údaje atp.), k tomu útočník využívá důvěřivosti své oběti. Sociotechnika je tedy prostředkem k získání cenných údajů, které mohou později sloužit ke krádeži identity, přístupu do chráněného systému nebo mohou být samy o sobě použity například pro marketingové účely.

Sociotechnika manipuluje s lidskou psychikou a je vázána na um osoby útočníka, jeho jednání a přesvědčovací talent, čímž se podobá výše uvedeným typům rizikového chování (zejména potom kybergroomingu). Zároveň však sociotechnika často využívá i technické prostředky, o nichž bude řeč dále v práci.

Pokud bychom chtěli sociální inženýrství nějak klasifikovat, můžeme jej dělit dle použitého média – může být vedené pomocí telefonu (vishing), dokonce může být cílem útoku přímo telefonní linka respektive její bezplatné použití (phreaking). [35] Další typy sociotechniky mají také základ ve fyzickém světě, tedy klasické koukání přes rameno (shoulder surfing), které může být dovedeno k dokonalosti např. sledováním, co uživatel dělá na počítači skrze kameru. [36 s. 145–146] Důvěrné informace může útočník hledat i mezi odpadem, takový útok se nazývá thrashing nebo též dumster diving. [34] Pro potřeby této práce bude zcela stěžejní zabývat se útoky vedenými za použití média internetu, mezi takové řadíme phishing, kterému je věnována celá další podkapitola.

4.2 Phishing

4.2.1 Základní charakteristika

Jak již bylo řečeno výše, phishing je druh sociotechnicky, která je na internetu velmi rozšířená, server `HOAX.cz` tento jev definuje jako *„podvodné e-mailové útoky na uživatele internetu, jejichž cílem je vylákat důvěrné informace.“*. [37] Do češtiny lze tento fenomén přeložit jako “rhybolov”, o útočnících se mluví jako “rhybářích”, což odpovídá I etymologii slova phishing z angličtiny – fishing = rybaření, Satrapa ve svém článku na serveru `Lupa.cz` překládá pojem ještě malebněji jako „rhybhářství“, v současné době se však používá překlad první. [38] Samotná podstata této techniky připomíná právě rybolov – útočník rozhodí sítě

(v tomto případě rozešle podvodné e-maily, které např. vyzývají k potvrzení přihlašovacích údajů) a čeká, která ryba (uživatel) se na takový útok chytí a údaje vyplní.

4.2.2 Phishing v číslech

Právě počet chycených „rhyb“ tedy uživatelů ukazuje, nakolik je tato technika oblíbená a účinná. Společnost Thrusteer uvádí, že 0,47 % klientů bank podlehne phishingu [39 s. 2], Florêncio a Herley spočítali, že phishingovým útokům ročně podlehne 0,4 % uživatelů. [40 s. 2] V absolutních číslech, které vyjadřují ztráty, které ročně vznikají právě v důsledku phishingoých útoků se celá skutečnost jeví ještě dramatičtěji. V roce 2006 byly ztráty způsobené phishingem v USA vyčísleny na 2,8 mld. USD [41], zajímavá jsou i čísla, která jsou aktuálnější a pocházejí z exotičtějšího prostředí, v roce 2010 činily ztráty způsobené phishingem v Číně 20 mld. Juanů [42], což je zhruba 60 mld. Kč (dle aktuálního kurzovního lístku ČNB ze dne 2. 4. 2012). Phishing je sice v posledních letech spíše na ústupu soudě podle klesajícího počtu útoků a svůj vrchol v roce 2009 již pravděpodobně nepřekoná, ale techniky, které používá, se stále zdokonalují a způsobené ztráty jsou stále enormní. [43 s. 5] Ačkoliv celkový počet útoků klesá, dochází ke specializaci útoků a ty jsou více šité na míru (působí tedy důvěryhodněji), jedná se o to takzvaný „spear phishing“. [44]

Česká republika má ve srovnání se zahraničím tu výhodu, že je malá a čeština je společným jmenovatelem pouze pro několik milionů obyvatel, útok na takové cíle není z mezinárodního hlediska tak výhodný, navíc jazyková bariéra celkem spolehlivě „blokuje“ většinu běžných útoků v angličtině a útoky s použitím automatického překladače jsou potom velmi podezřelé a snadno rozpoznatelné. I přesto jsme u nás byli svědky phishingových útoků např. na klienty České spořitelny, které se postupem času výrazně zlepšovaly. [45]

4.2.3 Běžné phishingové metody

Je možné najít mnoho různých metod, jak phishing uskutečnit, Emigh uvádí mezi různé varianty phishingu například i pharming (dále v práci má věnovanou podkapitolu 5.4) nebo phishing založený na *malwaru* – využití škodlivého programu nacházejícího se v počítači oběti (např. pomocí keyloggerů, viz podkapitola 5.3). [46 s. 6–12] V této podkapitole se budeme věnovat spíše technikám sociálního inženýrství ve spojení s e-mailovou komunikací, další technické možnosti, jak získat cizí identitu či osobní údaje jsou nastíněny dále (kapitola 5), ačkoliv jejich příbuznost s phishingem je zřejmá či jej rozvíjí.

Pro potřeby analýzy používaných phishingových metod využijeme běžný nekvalitní phisingový e-mail slibující pohádkovou výhru (dále označený jako e-mail č. 1), který pochází z mého archivu (příloha C) a vysoce kvalitní a detailně rozebraný phishingový e-mail

z archivu APWG, jehož cílem je zisk přihlašovacích údajů do elektronického bankovnictví (dále označovaný jako e-mail č. 2). [47] Pokusíme se najít společné jmenovatele či naopak ukázku rozdílných technik:

1. Padělaná hlavička zprávy s využití e-mail spoofingu (v detailu se mu věnuji dále v podkapitole 5.1.4).
    a. Odesilatel (`From`) – toto pole je padělané i u těch nejprimitivnějších phishingových zpráv, má navodit pocit, že Vám píše ověřená autorita (v analyzovaných případech se jedná o banku Sun Trust a server `Oil.com`).
    b. Adresa pro odpověď (`Reply-to`) – v případě phishingové zprávy č. 1 je odpověď žádoucí, proto je v hlavičce uvedena sběrná adresa (nekorespondující s odesilatelem), v případě č. 2 je adresa pro odpověď kopírovaná z padělaného odesilatele, údaje jsou z uživatele vylákány jiným způsobem.
2. Jazyk – u č. 1 se jedná o automaticky generovaný překlad, který navíc ani nepoužívá vhodnou jazykovou sadu. Č. 2 je potom anglicky (i to by bylo u nás velmi podezřelé). Nicméně i ke zprávám s perfektní češtinou je potřeba přistupovat obezřetně, protože v případě České spořitelny se phishingové zprávy v průběhu času výrazně zlepšily.
3. Design – zpráva je často doplněna logy a stylem instituce, kterou napodobuje (č. 2) u méně zdařilých zpráv se to neobjevuje (č. 1).
4. Odkazy – u phishingových e-mailů je uživatel často nabádán, aby pokračoval dále a potvrdil své přihlašovací údaje, toho docílí kliknutím na odkaz, který zdánlivě vede na stránku autority (banky). Obvykle se však jedná o odkaz na podvodnou stránku s firemním designem a podobně vypadající adresou. V případě č. 2 bylo ovšem použito metody XSS (už byl zmíněn v souvislosti s portálem `Facebook.com`), která v odkazu obsahuje zakódovaný odkaz na skript, který se provede a pravděpodobně poslouží k zachycení údajů zadávaných uživatelem. V případě č. 1 útočník spoléhá na pouhé přeposlání osobních údajů uživatele e-mailem s vidinou pohádkové odměny.
5. Útok na psychiku uživatele – phishingové zprávy dávají ultimáta, nutí uživatele rozhodnout se ihned, případně dávají nabídky příliš dobré na to, aby mohly být pravdivé. Č. 1 slibuje pohádkovou výhru, stačí zaslat jen pár osobních údajů, klasické útoky na platební služby (č. 2) obvykle hrozí zablokováním karty či účtu, odvrátit to lze jen okamžitým potvrzením uživatelových údajů (a tedy předání těchto údajů útočníkovi).

4.2.4 Jak se phishingu bránit

Velmi kvalitně zásady prevence zpracoval již Satrapa ve svém „desateru“. [48] Pokud bychom měli shrnout v kostce principy ochrany proti phishingu, případně přidat některé další, vypadal by bodový návod vycházející z lidové moudrosti asi takto:

1) Nedůvěřuj, prověřuj. *Každá zpráva může být podvod, zvaž všechna fakta, hledej další informace.*

2) Líná huba holé neštěstí. *Nestal se již někdo obětí podobného podvodu, není již podobný e-mail někde zaznamenán a zpracován, vždy můžeš zavolat na zákaznickou linku a zeptat se (kontakt hledej mimo podezřelou zprávu)?*

3) Příliš dobré než aby to byla pravda? Podvod. *Myslíte, že by Vám rozhodnutí o výhře několika milionů přišlo e-mailem v lámané češtině?*

4) Všechny cesty nevedou tam, kam to vypadá. *Padělat odesilatele i odkazy je velmi snadné, buď na pozoru, než někam klikneš, dvakrát si to rozmysli, hledej i jiné cesty, jak se dostat na místo určení (napiš odkaz ručně)!*

5) Vše má svůj čas. *Nenech se stresovat ultimáty, která ti pisatel dává.*

5 Technické metody útoku

5.1 Spoofing

5.1.1 Princip

Typů spoofingu existuje celá řada a každý z nich je v lecčem jedinečný, jejich společným jmenovatelem je snaha o maskování skutečných údajů. Útočník maskuje skutečnou adresu tak, aby vypadala, že pochází z důvěryhodného zdroje. Druh adresy, kterou útočník maskuje, závisí na typu spoofingu, který se liší jak technikou útoku, tak náročností provedení. Na internetu mezi nejčastější patří:

1) IP spoofing,
2) DNS spoofing,
3) E-mail spoofing.

5.1.2 IP spoofing

Slabina, která dovoluje útočníkovi použít tuto metodu, pramení přímo z návrhu TCP/IP. Útok spočívá v nahrazení skutečné adresy odesilatele v hlavičce v IP diagramu za adresu podvrženou. Tímto útočník může přesměrovat tok dat od uživatele směrem k sobě, místo, aby je uživatel posílal na server, jak se domnívá. V druhém kroku musí útočník obelstít i protokol transportní vrstvy TCP, ta na rozdíl od IP funguje na bázi spojované služby a v hlavičce obsahuje bajty, které udávají pořadové číslo prvního bajtu tohoto paketu (sequence number), které se shoduje s potvrzovacím číslem (acknowledgement number) předchozího paketu a právě to musí útočník správně odhadnout, aby spojení mohl úspěšně „uloupit“ a přesměrovat na sebe (díky změněné IP adrese odesilatele).

Matthew Tanase ve svém článku IP spoofing dělí na několik dalších poddruhů [49]:

1) Blind Spoofing, tedy spoofing naslepo, spočívá v odhadování potřebných údajů v hlavičce TCP datagramu.
2) Non-blind spoofing, neprobíhající „naslepo“, kde útočník číhá na stejné podsíti jako oběť a je tedy možné, aby potřebné údaje odposlechl.
3) Man in the Middle (MitM) jednoduše spočívá v tom, že se někdo usadí uprostřed spojení mezi serverem a klientem. Může pouze naslouchat nebo jednomu či druhému podsouvat údaje, o kterých si bude příjemce myslet, že pochází od skutečného partnera.
4) Denial of Service (DoS), česky nazývané odmítnutí služby, je v současné době asi mediálně nejznámějším typem útoku, který využívá IP spoofingu, jeho princip je vel-

mi primitivní: Útočník bombarduje server množstvím paketů, které díky IP spoofingu vypadají, jakoby pocházely od různých uživatelů, a proto je těžké takový útok zastavit a vystopovat. Zvláště v poslední době o podobných útocích slyšíme v médiích často, jedná se koordinované a distribuované útoky tohoto střihu (DDoS), jejichž cílem je zahltit a shodit server. [50] Nejedná se tedy o útok s cílem získat osobní údaje či jiná data o uživateli.

5.1.3 DNS spoofing

Tato metoda je často spojována s technikou, která se nazývá pharming (která je popsána v podkapitole 5.4). Útok je veden na překlad doménového jména na IP adresu. Uživatel do prohlížeče napíše adresu serveru, na který chce přistoupit např. `www.mbank.cz`. Nedojde však k překladu na IP adresu požadovaného serveru, tedy mBanky, ale na jinou adresu, kterou si zvolil útočník.

DNS spoofing může být realizován dvojím způsobem, buďto infikováním routeru, do kterého se podařilo útočníkovi proniknout (třeba díky nezměněnému nebo slabému heslu routeru). Druhou možností, je provést DNS spoofing lokálně přímo v operačním systému počítače, ve Windows by se jednalo o přepsání záznamů souboru `hosts`, modifikaci souboru by potom útočník mohl provést podstrčením vhodného malwaru uživateli např. trojského koně. [51]

5.1.4 E-mail spoofing

V porovnání s ostatními druhy spoofingu je e-mail spoofing zdaleka nejjednodušší, velmi často se s ním lze setkat v rámci phishingových zpráv. Jeho princip spočívá v nastrčení vhodných údajů do hlavičky e-mailu, aby vše budilo co možná největší důvěru příjemce. Nejčastěji se v hlavičce e-mailu padělá adresa odesilatele, včetně jména (`From`) a cesty, kterou e-mail putoval (`Received`). První jmenovaná technika má za cíl navodit u uživatele pocit, že e-mail pochází od skutečné autority, napsala Vám ho skutečně Vaše banka. Druhá technika je potom ochranou před SPAM filtry. [47 s. 4]

K posílání zpráv s padělanou hlavičkou útočník nepotřebuje žádných zvláštních prostředků, ani znalostí, základní návod k tvorbě takovéhoto e-mailu se vejde do několika minutového videotutoriálu či jednoduché prezentace. Docílit toho lze například pomocí síťového protokolu telnet sloužícího pro emulaci terminálu u sítí na bázi TCP/IP. [52 s. 5–6] Útočník otevře spojení se serverem, který obsluhuje poštu pro danou doménu (MX záznam pro jednotlivé servery lze pohodlně získat například pomocí nástroje Domain Dossier na stránce

`www.centralops.net`), serveru potom dle pravidel SMTP komunikace poskytne potřebné informace (odesilatel, příjemce, tělo zprávy). Server následně doručí na cílovou adresu vše, co uživatel zadal, nedochází k žádnému ověřování pravdivosti údajů.

5.2 Spyware

„Spyware je program v počítači, jenž bez vědomí uživatele odesílá data přes internet.“. [53] Takováto definice je asi nejjednodušším možným popsáním malwaru, který je cílen na zaznamenávání údajů uživatele a jejich odeslání k útočníkovi. Takto získaná data potom mohou být použita k získání přístupových jmen a hesel k nejrůznějším účtům, dalších citlivých údajů a případně i dat, která mohou být použita k zasílání či lepšímu cílení reklamy (tzv. consumer profiling).

Spyware si může uživatel bezděčně nainstalovat do systému mnoha způsoby – použije program, který kromě funkce, ke které je primárně určen, má v sobě též zahrnutý škodlivý kód, který sbírá a posílá data o uživateli. K dalším možnostem šíření spywaru patří instant messengery (např. ICQ), peer-to-peer aplikace či infikované stránky.

5.3 Keylogger

Ke speciálním typům spywaru patří takzvané keyloggery, jejichž funkce spočívá v zaznamenávání úhozů do klávesnice infikovaného počítače a následné přeposlání dat útočníkovi. [54] Cílem takové aktivity je pochopitelně zachycení přihlašovacích jmen a hesel, která mohou být poté zneužita útočníkem ke krádeži identity či získání dalších osobních údajů. Shetty uvádí 3 typy keyloggerů: [54]

1) Hardwarové keyloggery jsou zařízeními umístněnými mezi klávesnici a počítač. Jako takové potřebují fyzický přístup k počítači. Do výše zmiňované definice spywaru je zahrnout nemůžeme (nejsou programy v počítači) a jejich pozice je tedy poněkud specifická.

Obrázek 5.1: Hardwarový USB keylogger

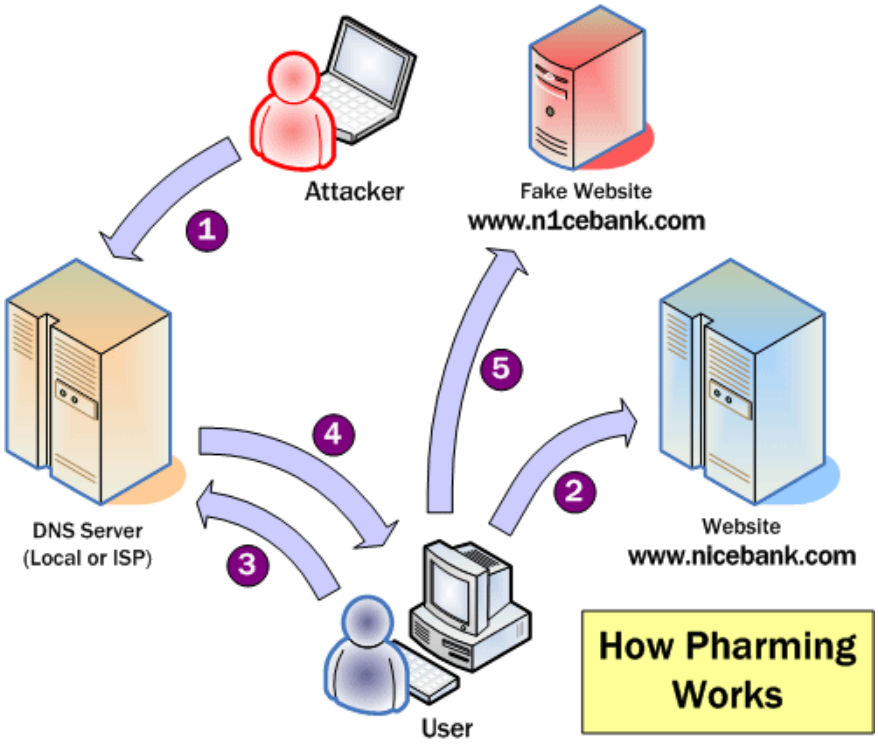
2) Softwarové keyloggery založené na „hákovacím“ mechanismu. Využívají funkci `Windows SetWindowsHookEx ()`, která společně s přidruženou dynamickou

knihovnou dokáže zaznamenávat veškeré úhozy do klávesnice včetně automatického vyplňování přihlašovacích údajů.

3) Jádrové nebo řadičové keyloggery jsou nad aplikační vrstvou (na rozdíl od předchozího typu keyloggerů) a jsou umístněny přímo na úrovni jádra a úhozy zaznamenávají přímo z klávesnice či jiného vstupního zařízení.

5.4 Pharming

Tato metoda je založena na principu DNS spoofingu (podkapitola 5.1.3) a kromě technického řešení do jisté míry vykazuje i jevy sociotechniky a podobá se phishingu, proto ji Ondřej Bitto nazývá *„mladším sofistikovanější a hlavně nebezpečnějším bratříčkem phishingu.“*. [51] Jak již bylo popsáno v 5.1.3, uživatel je po zadání jmenné adresy přesměrován na jinou stránku a zde již do jisté míry přichází ke slovu sociotechnická část – uživatel musí být neustále v přesvědčení, že se nachází na jím požadované stránce. Stránky tedy vypadají často velmi identicky, uživatel má tedy velmi malou šanci odhalit, že se stal obětí podvodu a přihlašovací údaje např. internetového bankovnictví zadá. Do jisté míry lze takové stránky rozpoznat např. kvůli absenci zabezpečeného HTTPS spojení potvrzeného příslušným certifikátem. Celkové schéma toho, jak pharming funguje, je uvedeno na obrázku 5.2.



Obrázek 5.2: Schéma toho, jak funguje pharming

6 Prostředky zabezpečení

6.1 Obecné zásady

Veškeré materiály zaměřené na ochranu počítače před malwarem, ať už určené pro děti či dospělé vždy obsahují základní trojici doporučení:

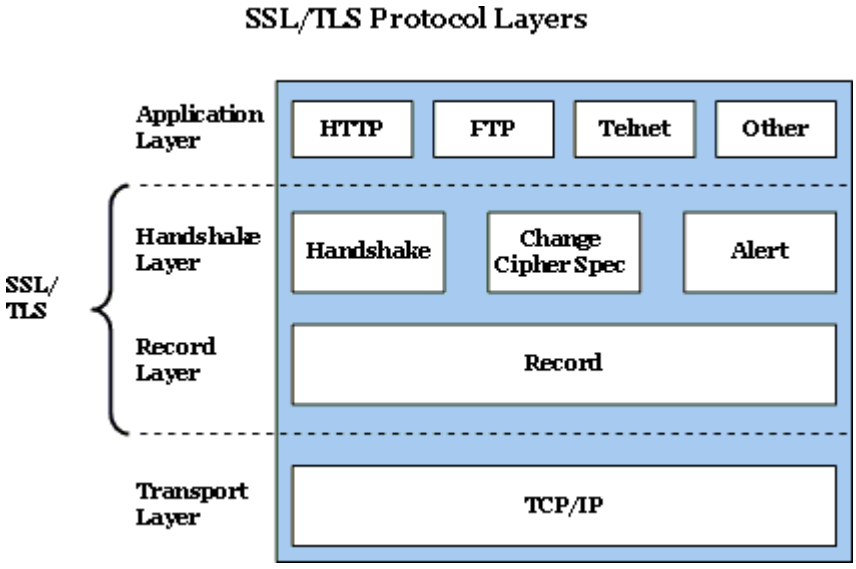
1) Používejte pouze legální programy a operační systém a pravidelně OS aktualizujte.
2) Používejte firewall, ten samozřejmě musí být také správně nakonfigurovaný, protože jinak jeho ochranná funkce klesá.
3) Používejte vhodný antivirový program a pravidelně ho aktualizujte (povětšinou se o to postará za Vás). Antivirový program může být doplněn i o vhodný antispywarový program či další komponenty (např. antiadwarové programy atd.).

V souvislosti s osobními údaji, jejich ochranou a zneužitím je dále potřeba se hlouběji věnovat problematice hesel, jejich síle a výběru. Dalším aspektem, který nemůže být opomenut, je zabezpečená (šifrovaná) komunikace například pomocí protokolu HTTPS. I elementární znalost, porozumění a aplikace výše zmiňovaných okruhů výrazně zvyšuje bezpečí uživatele a jeho údajů.

6.2 Šifrované protokoly

Základní verze aplikačního protokolu HTTP (hypertext transfer protocol) neumožňuje komunikaci šifrovat, a proto je velmi náchylná k odposlechu. Tento problém bezpečnosti je vyřešen v HTTPS (hypertext transfer protocol secure), opět se nešifruje na aplikační vrstvě. Klasický model protokolu TCP/IP ani neumožňuje šifrovat na transportní vrstvě, proto k šifrování dochází mezi těmito vrstvami a to pomocí SSL (secure sockets layer) respektive pro Internet se jedná o TLS (Transport layer security protocol), který ze zmíněného SSL vychází. [52 s. 389–391] Obrázek 6.1 přehledně zobrazuje jednotlivé „horní“ vrstvy a vysvětluje, o jaké prvky je HTTPS bohatší oproti nešifrovanému HTTP.

SSL (resp. TLS) funguje na bázi klient-server a šifruje informace mezi oběma subjekty, díky čemuž není možné odposlouchávat, respektive rozumět odposlechnuté komunikaci. Vrstva SSL/TLS přináší v bezpečnosti jakousi další úroveň, jak Dostálek vysvětluje: *„Vrstva SSL/TLS provádí autentizaci za využití certifikátů, kdežto protokol HTTP provádí základní autentizaci např. jménem a heslem.“*. [52 s. 414] Vrstva SSL/TLS tedy původní bezpečnostní prvky nenahrazuje, ale přidává jim bezpečný kanál, po kterém mohou být přenášeny. V praxi se ve většině případů využívá pouze certifikátu na straně serveru, ale je z principu možné certifikát přidělit i klientovi.



Obrázek 6.1: Schéma vrstev SSL/TLS

HTTPS se hojně využívá při přihlašování do nejrůznějších aplikací. Zatímco například webová rozhraní pro internetové bankovnictví ho využívají bez výjimky, při přihlašování do aplikací jako je Facebook či webmail na `Seznam.cz` je zapnutí HTTPS (respektive šifrování přes SSL/TLS) pouze volitelné a je v základním nastavení vypnuto. Prohlížeče na přechod do HTTPS módu reagují zvýrazněním dané skutečnosti (barevně, ikonou zámečku, nápisem zabezpečené…), tento jednoduchý fakt mohou vnímat i uživatelé začátečníci a ve chvíli, kdy se mají nacházet na přihlašovací stránce pro internetové bankovnictví a komfort HTTPS jim „není dopřán“, měli by zbystřit, zda se nestali oběťmi podvodu (např. pomocí DNS spoofingu, či zda nenaletěli na phishingovou zprávu).

6.3 Hesla

6.3.1 Běžná uživatelská praxe

Lze konstatovat, že nešvary při tvorbě hesel se za posledních 20 let nezměnily, jak dokazuje studie Impervy z roku 2010. [55 s. 2] Pokud se opřeme o výzkum

Florêncía a Herleye získáme následující vhled do struktury uživatelských hesel a jejich použití: [40 s. 1]

1) Uživatel má v průměru 6,5 různého hesla.
2) Každé heslo je v průměru použito zhruba pro 3,9 rozdílné stránky.
3) Každý uživatel je v průměru vlastníkem zhruba 25 různých účtů.

O jejich skutečné síle a odolnosti proti případným útokům nám toho mnoho vypoví únik 32 milionů hesel z prosince roku 2009 ze stránek `Rockyou.com`. [55 s. 1] Tato společnost se zabývá výrobou a provozem online her (mimo jiné i známých farmářských her na Facebooku), které se těší značné oblibě u dětí a mládeže – čímž jsou dále uváděná zjištění velmi relevantní vzhledem k obsahu této práce. Skutečná uživatelská praxe se ukázala jako obrovský problém bezpečnosti. Specialisty z Impervy bylo zjištěno, že téměř 16 % uživatelů použilo pouze číselného hesla, dále bezmála 42 % uživatelů použilo hesla, která obsahují pouze malá písmena. 30 % uživatelů použilo hesla o délce menší než 6 znaků a téměř 70 % všech hesel bylo kratších jak 8 znaků. [55 s. 3] Tabulka 6.1 uvádí 20 nejčastěji používaných hesel. Míra jejich bezpečnosti je přinejmenším problematická, při použití slovníkového útoku s těmito hesly by případný útočník byl velmi úspěšný. Imperva spočítala, že za 17 min takového útoku přes síť (ačkoliv rychlost, kterou uvádějí u útočníka pro upload – 55 KB/s, je dnes již velmi často překonaná, například základní připojení, které nabízí společnost UPC má zhruba dvojnásobnou rychlost [56]) by získal 1000 účtů. [55 s. 4]

Pokud bychom získali náhled na hesla používaná českými uživateli, je velmi pravděpodobné, že bychom na horních příčkách nejpoužívanějších hesel našli kromě číselných řad i heslo „heslo“ či oblíbená dívčí jména, která byla v kurzu před více jak 20 lety stejně jako jsou nyní. [57]

Pořadí	Heslo	Četnost
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Pořadí	Heslo	Četnost
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

Tabulka 6.1: Top 20 nejoblíbenějších hesel uživatelů serveru `Rockyou.com`

6.3.2 Metody útoku

Pokud se bude útočník pokoušet prolomit heslo, má na výběr z více možností, jak takový útok provést a stále rozšiřující se základnu nástrojů, které mu to umožňují. Příkladem takového programu je L0PTHCRACK, který je navržen tak, aby byl nejen programem pro správu hesel, ale aby je dokázal i prolamovat.

Výpočetně nejsložitějším typem útoku je takzvaný útok *hrubou silou* (brute force), ten spočívá v použití všech možných kombinací znaků, které by mohly být pro heslo použity. S tímto typem útoku je možné dané heslo zjistit vždy, ale zisk takového hesla v reálném čase pro hesla o větším počtu znaků není možný. Druhou proměnnou je set znaků, které budeme používat, zatímco zjišťovaní hesla, které bude složené pouze z číslic, bude velmi rychlé, použití zvláštních znaků a velkých písmen dobu prolamování mnohonásobně prodlouží. Třetí proměnnou je výpočetní výkon použitého počítače, rychlý dvouprocesorový počítač dokáže 7 znakové heslo složené pouze z malých písmen abecedy (26 znaků) se 100% jistotou prolomit za 13 min. Stejně dlouhé heslo složené z číslic, malých a velkých písmen (62 znaků) však prolomí až zhruba za 4 dny. [58] Je patrné, že tento druh útoku funguje pouze do jisté síly hesla, poté dochází k neúměrnému prodlužování doby a silná hesla nelze ani s použitím nejmodernější výpočetní techniky prolomit v reálném čase.

Sofistikovanějším druhem útoku je takzvaný *slovníkový útok*, který využívá databázi slov, která zkouší. Lidé často tíhnou k tomu využívat jako hesel existujících pojmenování a právě této lidské slabosti se využívá při tomto druhu útoku. Oproti útoku hrubou silou dokáže prolomit i velmi dlouhá hesla za velmi krátký čas, jeho nevýhoda ovšem spočívá v tom, že nevyzkouší zdaleka všechny možnosti a pokud uživatel zvolil jinou než slovníkovou frázi nebo ji modifikoval, takový útok nemůže heslo zjistit.

Další možnosti dává útok využívající permutací slov a čísel a řeší tak některé nejčastější případy úpravy slovníkových výrazů. [59 s. 27] Tento typ útoku, též někdy nazývaný *hybridní* dokáže prolomit i hesla, se kterými si slovníkový typ útoku neporadil a zároveň se jedná o velmi časté a jednoduché úpravy lexikálních výrazů čísly např. „pr0ton“ či „osel4“.

Jako čtvrtý typ útoku uvádí Yan *útok s využitím osobních informací*. [59 s. 27] Takovýto útok můžeme často vidět zejména v detektivních a akčních filmech, kde hrdina uhádne heslo na základě znalosti osoby, které heslo patří – může se jednat o jméno psa, datum narození dcery, či název oblíbeného obchodního řetězce. K provedení je potřeba mít dobrou znalost o subjektu, kterému je heslo prolamováno a takovýto útok je tedy použitelný u cílených pokusů o prolomení hesla u konkrétní osoby. Je paradoxní, že k průniku jsou použity osobní

údaje, o jejichž ochranu je usilováno, ale v současné době jsou zároveň často lehkovážně poskytovány na internetu.

6.3.3 Tvorba bezpečného hesla

Obecně lze tvrdit, že bezpečným heslem je takové, které dokáže bez problémů odolat výše uvedeným typům útoku (i velmi intenzivním). Tedy heslo dostatečně dlouhé, které obsahuje speciální znaky, číslice, velká i malá písmena. Dále se nejedná o žádný údaj spojený s osobou majitele hesla a taktéž se nejedná o mírně upravený či neupravený slovníkový výraz (reálné slovo či vlastní jméno).

Jako vhodný kandidát na takové heslo se tedy jeví náhodně generované heslo (ať už počítačem či uživatelem) o dostatečné délce zahrnující speciální znaky a čísla. Tady ovšem narážíme na zásadní problém, který je také základním pilířem výzkumu Yanova výzkumu, tím je zapamatovatelnost pro uživatele. Ta je samozřejmě u takovéhoto hesla problematická. [59] Alternativou je heslo skrze klíčovou frázi zjednodušenou v heslo, např. „Mám jednoho mladšího bratra a dvě starší sestry“ můžeme zapsat takto: „M1mba2ss“. Takovouto klíčovou frázi si dokážou uživatelé zapamatovat v daleko kratším čase a snáze než je tomu u zcela náhodně generovaných hesel, přitom prolomitelnost takových hesel je stejná. [59 s. 29]

Další rady, kromě výše zmiňovaných, jsou velmi dobře a přístupně shrnuty na stránkách `ConnectSafely.org`, patří mezi ně pravidla pro uchovávání hesel – nikdy je nikomu nesdělovat a pokud si je musíme zapsat, potom takový záznam uchováváme na bezpečném místě, taktéž by neměl uživatel využívat totožná hesla pro více stránek. [60]

6.3.4 Vícefaktorová autentizace

V předchozí podkapitole 6.3.3 jsme se věnovali pouze jednomu aspektu autentizace, ačkoliv je zdaleka nejběžnějším, existují i další typy, které se často právě společně kombinují, aby bylo dosaženo maximální bezpečnosti. Takováto opatření jsou běžným zabezpečením například internetového bankovnictví. Metody autentizace můžeme dle FFIEC rozdělit do 3 kategorií, které se ve vícefaktorové autentizaci vzájemně kombinují: [61 s. 3]

1) Něco, co uživatel ví (heslo, PIN),
2) něco, co uživatel má (USB klíč, kreditní karta),
3) něco, čím uživatel je (biometrické charakteristiky, např. otisk prstu).

Internetové bankovnictví České spořitelny kombinuje znalost přihlašovacího jména a hesla (něco, co ví) s potvrzováním za použití mobilního telefonu majitele účtu (něco, co má).

7 Vzdělávací politika a ochrana osobních údajů

Vzdělávací politika má za cíl pružně reagovat na měnící se svět a zahrnovat mezi obsahy vzdělávání i aspekty informačních a komunikačních technologií. Nedílnou součástí ICT je i ochrana osobních údajů a zodpovědné chování v online světě. Je tedy nezbytné, aby byli žáci učeni i takovým znalostem, dovednostem a postojům, které jsou s tématikou ochrany osobních údajů spojené.

7.1 Rámcový vzdělávací program pro základní vzdělávání

Nejnovější dokument české státní vzdělávací politiky RVP ZV z roku 2007 [62 s. 104] ukládá, aby během základního vzdělávání žák absolvoval celkem 2 hodiny informačních a komunikačních technologií (vzdělávací obor). 1 hodina je určena pro 1. stupeň a 1 hodina pro 2. stupeň. Ochranu osobních údajů bychom mohli spatřovat v cíli „*učit žáky aktivně rozvíjet a chránit fyzické, duševní a sociální zdraví a být za ně odpovědný.*“. [62 s. 13] Pod pojmem sociální zdraví můžeme spatřovat i cíl „účinně si chránit soukromí“. V klíčových kompetencích můžeme „zdravé komunikační návyky online“ spatřovat jako součást kompetence komunikativní *„využívá informační a komunikační prostředky a technologie pro kvalitní a účinnou komunikaci s okolním světem.“*. [62 s. 15]

Pokud se detailněji zaměříme na vzdělávací oblast informační a komunikační technologie se stejnojmenným oborem, můžeme v očekávaných výstupech pro 1. stupeň nalézt formulaci: *„chrání data před poškozením, ztrátou a zneužitím“*. [62 s. 35] Právě zneužití osobních údajů je relevantní k tématu této práce v rámci tohoto očekávaného výstupu lze žáky naučit jak vytvářet hesla, chránit své osobní údaje a komunikovat bezpečně online. Ke komunikaci se taktéž váže očekávaný výstup: *„komunikuje pomocí internetu či jiných běžných komunikačních zařízení.“* [62 s. 35] a v rámci učiva uvádí komunikaci přes e-mail či chatovací servery, součástí výuky takové komunikace by měly být i zásady bezpečnosti komunikace (manipulace pomocí sociálního inženýrství, riziková komunikace atp.).

Na druhém stupni již nacházíme pouze očekávaný výstup: *„ověřuje věrohodnost informací a informačních zdrojů, posuzuje jejich závažnost a vzájemnou návaznost“*. [62 s. 36] Mezi učivem nalezneme pojem Internet – v rámci tohoto očekávaného výstupu lze vyučovat i o nebezpečí, které představují phishingové zprávy a jiné metody sociotechniky.

Rámcový vzdělávací program nám nabízí prostor pro začlenění výuky o ochraně osobních údajů na internetu do učiva a můžeme rozpoznat, že porozumění tomu, jak se „bezpečně chovat online“, je očekávaným výstupem. Na stranu druhou nám RVP svými obecnými formulacemi nedává jistotu, že je to tak skutečně myšleno. Nacházíme zde zmínky o chatech,

ale problematika sociálních sítí RVP zcela uniká a to včetně nově navrhovaného RVP z roku 2010. [63] S jistou dávkou fantasie lze do klíčových kompetencí a očekávaných výstupů zařadit téměř libovolnou pozitivní znalost, dovednost či postoj, kterou si žák vytvoří. Ochrana osobních údajů či riziková komunikace nejsou jako takové v dokumentu zmíněny vůbec a jejich zařazení do učiva je tak věcí nejistou, ačkoliv se jedná o souhrn znalostí, dovedností a postojů s důrazem zejména na postojovou složku, které je důležité, aby si žák osvojil a přijal za své.

V optimálním případě by většinu znalostí, dovedností i postojů měli žáci získat již na 1. stupni. 2. stupeň by měl pouze rozvinout znalosti o kvalitě informací a případných metodách sociotechniky. Rozvíjeny by měly být i dovednosti, jak takové metody útoku poznat. Vše by mělo být provázáno se skeptickým postojem k obsahu Internetu spojeným s ověřováním pravdivosti informací, které se tam nalézají.

7.2 Školní vzdělávací programy vybraných škol

Pro bližší analýzu ŠVP byly vybrány dvě školy, na nichž bylo následně realizováno prohloubené dotazníkové šetření a aplikace vzdělávacích materiálů, které jsou součástí praktické části práce. První školou je Gymnázium, Jablonec nad Nisou, U Balvanu 16, příspěvková organizace se vzdělávací programem pro nižší gymnázia, druhou analyzovanou školou byla ZŠ, Liberec, Aloisina výšina 642, která vyučuje dle ŠVP pro ZŠ.

Na výše uvedeném gymnáziu celková hodinová dotace pro vzdělávací oblast informační a komunikační technologie činí 3,5 hodiny a výuka je realizována v 8. a 9. ročníku. Tématika ochrany osobních údajů a zejména dat je uvedena v očekávaném výstupu 9. ročníku (kvarty): „*orientuje se v systému programů pro ochranu dat a dokáže s některými z nich pracovat (antivirový software, ...)*“. [64 s. 77] V rámci učiva k tomuto očekávanému výstupu je uváděno toto*: „Ochrana dat, programy pro ochranu dat a pravidla pro bezpečnou práci s internetem*“. [64 s. 77] Takto definované učivo odpovídá obsahu této práce, nicméně je zde cítit důraz, který je kladen na technickou stránku ochrany dat a ne už tolik na postoje spojené s ochranou osobních údajů a jevy rizikové komunikace. To je v souladu s RVP a výukou informačních a komunikačních technologií na 2. stupni ZŠ. Předpokládá se tedy již jisté osvojení těchto znalostí, dovedností a postojů během studia na 1. stupni ZŠ. V rámci realizace očekávaného výstupu, který jsem výše citoval, je zmíněno i průřezové téma mediální výchovy, tomu se okrajově věnuje analýza výukových materiálů (kapitola 8).

ZŠ Aloisina výšina má 2 hodiny informačních a komunikačních technologií povinné a to v 5. a 6. ročníku, dále v 7.–9. ročníku nabízí 2 hodiny informačních a komunikačních

technologií týdně jako povinně volitelný předmět. Ochraně osobních údajů se věnuje ŠVP zejména v 6. ročníku v rámci tématu „Internet“. V učivu je uveden e-mail a chatovací servery (tedy práci s nimi, pravidla i rizika), mezi očekávané výstupy zařazují: *„Použije PC jako zdroj zábavy a odpočinku.“* [65] Toto tvrzení naprosto realisticky ilustruje zájmy žáků a oblast, kde by se mělo zejména působit s ohledem na ochranu osobních údajů a rizikovou komunikaci.

8 Výukové materiály s tématikou ochrany osobních údajů

8.1 Učebnice

Lze obecně říci, že učebnice určené k výuce informačních a komunikačních technologií se tématice ochraně osobních údajů příliš nevěnují. Pokud ano, tak spíše okrajově či v nedostatečné šíři. Učebnice, které se alespoň částečně takové problematice věnují, jsou zde uvedeny a obsah je shrnut.

Informatika 3 pro ZŠ a víceletá gymnázia věnuje počítačové kriminalitě 2 stránky a to zejména s důrazem na technické aspekty ochrany, případně tvorbu a péči o hesla, o zbylých nebezpečích se letmo zmiňuje v několika větách. [66 s. 95–96]

Informatika pro základní školy 2. díl se osobním údajům věnuje na půlce stránky v podkapitole o soukromí při chatování, dále se zde objevují také zásady při používání internetového bankovnictví a učebnice varuje před podvodnými zprávami na další polovině strany. [67 s. 10–12]

Učebnice Tvorivá informatika věnuje hrozbám na internetu kapitolu počítač a (ne)bezpečnosť. Ač má kapitola pouze tři stránky snaží se alespoň bodově a zajímavou formou upozorňovat na rizika spojená s používáním počítače, využívá k tomu myšlenkových map či otázek k zamyšlení. Zpracování učebnice podporuje další diskuzi těchto témat. [68 s. 40–42]

Tématika osobních údajů je velmi dobře rozpracována v učenici Mediální výchova v kapitole nová média, kde se autoři věnují i fenoménu sociálních sítí a dalších komunikačních kanálů (ICQ, Skype…), který v ostatních učebnicích není reflektován. Kapitola informuje o bezpečnosti informací na internetu – hesla, sociotechnika a to včetně aspektů rizikové komunikace. Série nabízí v rámci cvičebnice i diagnostické materiály a cvičení, v metodice jsou popsány i další náměty pro aktivity a diskuzi o problematice. [69] [70 s. 46–48, 86–87] [71 s. 95–101]

V rámci průřezového tématu mediální výchovy se v Základech mediální výchovy setkáváme s kapitolou věnovanou komunikaci a seznamování přes internet s názvem „Láska přes internet“, která se věnuje chatování, jeho výhodám a nevýhodám, poskytování osobních údajů a taktéž kybergroomingu. Jedná se o kapitolu velmi úzce specializovanou, ale velmi kvalitně připravenou pro využití v hodinách informačních a komunikačních technologií. [72 s. 157–163]

Obecně lze tvrdit, že hrozbám, které internet skýtá je věnováno zejména v tuzemských učebnicích pro informační a komunikační technologie poměrně málo místa, pokud se dále

omezíme na ochranu osobních údajů, je informací velmi poskrovnu nebo nejsou vůbec. Útočiště nalezlo téma v mediální výchově, kde je mu v rámci média internetu věnován prostor.

8.2 Webové portály

Jen u nás působí široké spektrum webových portálů, které se bezpečností na internetu zabývají. Jedná se např. o projekt kolem Univerzity Palackého a centra PRVoK, zejména portály E-bezpečí.cz [73] a derivát zaměřený pouze na sexting Sexting.cz [74], pro pedagogy je určen spřízněný portál E-nebezpečí.cz [75]. Tyto portály dávají velmi aktuální náhled do problematiky rizikové komunikace a dalších nebezpečí na internetu. Na portálech je možné najít jak odborné články či výzkumné zprávy Kopeckého a Krejčí z uplynulých let, tak materiály určené dětem, rodičům i pedagogům.

Dalším portálem, který se touto tématikou zabývá je portál Saferinternet.cz [76], který publikoval i výzkumné zprávy, je spojen taktéž s celosvětovou aktivitou Safer Internet Day. Tento portál je zřizován Národním Centrem Bezpečnějšího Internetu. Portálem, který má na svědomí stejný tým je i Bezpečně-online.cz [77]. Portály jsou opět cílené nejen na děti ale i rodiče či kohokoliv dalšího, kdo má zájem o tuto problematiku.

Dalším projektem je Bezpečnýinternet.cz [78], na jehož tvorbě se podílely pouze firmy z komerčního sektoru a jehož cílem je také zvýšit povědomí o rizicích na internetu zejména mezi dětmi a mládeží, také nabízí sekce pro rodiče i pedagogy. Tento portál je firmou Seznam.cz spojen i s portálem Seznamsebezpečně.cz[79] a filmem, který se zabývá tématikou rizikové komunikace a osobních údajů a těší se značné oblibě mezi pedagogy.

Taktéž ÚOOÚ má vlastní portál a sekci pro mládež. V rámci svých aktivit například pořádá soutěž „Moje soukromí! Nekoukat, nešťourat!“, která probíhá již od roku 2007. [80]

Na mezinárodním poli stojí za zmínku portál ConnectSafely.org [81] a jeho deriváty Safekids.com [82] cílený na děti a Safeteens.com [83] cílený na starší věkovou skupinu, dále Saferinternet.org [84], který je úzce spjat s naším národním portálem Saferinternet.cz. Portál zaměřený výhradně proti phishingu Antiphishing.org [85] má v rámci svých stránek velmi zajímavý projekt takzvané „přistávací stránky“ [86], která vysvětluje rizika phishingu. Princip této stránky tkví v tom, že správci sítí místo pouhého blokování phishingových stránek je přesměrují na tuto stránku, uživatel, který by se kliknutím na odkaz vedoucí na podvodnou stránku nachytal se ihned a bezpečně poučí o chybách, které udělal a jak málo chybělo, aby se stal obětí počítačové kriminality.

8.3 Videomateriály a komiks

V našem prostředí je velmi známe již zmiňované video „Seznam se bezpečně“ umístněné na stejnojmenném portálu, které je asi nejpoužívanějším videomateriálem k této problematice u nás. Velmi dobrým projektem se může pyšnit Slovensko. V rámci portálu `Ovce.sk` [87] jsou umístněny animovaná videa ze salaše, která hravou, alegorickou a moderní formou vysvětlují dětem různá rizika internetové komunikace, jako jsou kybergrooming, sexting či rizika sociálních sítí. I přes drobnou jazykovou bariéru by tato videa mohla být velmi přínosná při vysvětlování této problematiky žákům. Otitulkované filmy tohoto projektu existují v mnoha jazycích, v češtině však ne, což je škoda.

Komiksové zpracování látky je jednodušší a taktéž hojné, v našem prostředí se jedná o interaktivní komiksové příběhy na portálu `Bezpečnýinternet.cz`, které však obsahově i technicky zaostávají za některými mezinárodními počiny jako je například `Securitycartoon.com` [88], který obsahuje obrovské množství komiksových stripů, které se zabývají jak technickým zabezpečením počítače, tak sociotechnickou, jevy vysvětluje komiks velmi přesně odborně a zároveň přístupně i pro laiky, děti a mládež. Po profesionální stránce je z mého pohledu opravdu excelentně zvládnutý portál `Privacyactivism.org` [89] jehož součástí je i skvěle graficky vypadající komiks Network: Carabella od the Run, který skrze poutavý akční příběh ukazuje až dystopickou budoucnost sociálních sítí, součástí portálu jsou i materiály pro učitele a příručka jak s komiksem pracovat a využít jej jako vhodný materiál pro výuku.

Videomateriály a komiksy skýtají atraktivní formu, jak žákům přiblížit problematiku ochrany osobních údajů a jiných rizikových jevů na internetu. Kromě tvorby vlastních, obvykle technicky méně zdařilých počinů, by jistě za úvahu stálo i přeložení již existujících zahraničních materiálů do češtiny. V případě jazykově zdatných studentů (např. na středních školách) lze s materiály pracovat mezioborově v rámci anglického jazyka a informačních a komunikačních technologií.

9 Metody sběru dat

Nutnou součástí práce bylo zjištění výchozích znalostí žáků v oblasti ochrany osobních údajů na internetu a jejich změna v návaznosti na realizovanou výuku. Jednou z možností, jak zjistit tyto údaje, je i dotazníkové šetření – ideální nástroj pro získávání velkých objemů písemných odpovědí na výzkumníkem zadané otázky.

9.1 Výhody online dotazníkového šetření

Oproti klasickému dotazníkovému šetření skýtá sběr dat online mnohé výhody. Pro samotnou konstrukci dotazníku existují typově předem připravené otázky, např. zatrhněte více odpovědí (checkbox) nebo z následujících vyberte jedno (radio), ty automaticky vkládají vámi požadovaný prvek a navíc kontrolují, zda skutečně respondent neodpovídá v rozporu s instrukcemi (zatrhává více, pokud má zatrhnout pouze jedno atp.). Oproti klasickému dotazníku je navíc možno označit otázku jako povinnou a tím zamezit odeslání nekompletního dotazníku respondentem (bude upozorněn a nevyplněná otázka bude barevně označena). Online dotazník šetří i prostředky, které by bylo nutné vydat za tisk papírových dotazníků. Jeho distribuce probíhá odesláním odkazu, který vede na dotazníkový formulář, není potřeba dodatečné fyzické distribuce. Vyplnit dotazník může respondent kdekoliv, kde má přístup k internetu a kdykoliv během času, který je pro šetření určen. Dotazníkové šetření lze snadno ukončit a systém již potom další odpovědi nepřijímá.

Zpracování dat získaných prostřednictvím online dotazníků má také velké množství výhod, výsledky jsou ukládány ve formátu, který je snadno zpracovatelný tabulkovým procesorem a v závislosti na prostředí jsou k dispozici i nástroje, které provádějí statistické výpočty (průměry, odchylky, procentuální zastoupení jevů atp.).

9.2 Nástroje pro online dotazníkové šetření

Pro dotazníkové šetření v této práci byly využity nástroje pro tvorbu dotazníků, které jsou součástí Google Docs, mezi jejich přednosti patří jednoduchost, rychlý výběr vzhledové šablony a zároveň nástroje nepostrádají žádný ze základních prostředků pro tvorbu a zpracování otázek v dotazníku. Navíc je služba zcela zdarma, lze ji využívat jako součást Vašeho účtu na Googlu.

Další nástroje určené k online sběru dat, které stojí za pozornost, jsou servery `Vyplňto.cz` a `Formees.com`. `Vyplňto.cz` je hojně využívaný tuzemský server, je možné jej využívat zdarma, nicméně některé funkce jsou přístupné pouze pro prémiové uživatele. Za zmínku zde stojí nadstandardní statistické zpracování dat získaných z dotazníků,

nicméně v neplacené verzi chybí některé nástroje, bez nichž by tvorba dotazníku byla obtížná a těžkopádná.

Druhou alternativou je `Formees.com`, který nabízí kvalitní vývojové prostředí pro tvorbu dotazníků a umožňuje si vytvořit dotazník přesně na míru a dle vlastního designu. Verze zdarma nabízí širokou škálu nástrojů a pouze decentní reklamní banner. Po vyzkoušení se nicméně dospělo k rozhodnutí jej nepoužít, zejména protože nevyhovoval nástroj pro návrh dotazníku, a protože dotazník bylo potřeba rozčlenit do více listů.

II. Praktická část

10 Výukové materiály

10.1 Ukázková hodina

Jedním z cílů práce bylo vytvořit materiály a podklady pro ukázkovou hodinu, která bude použita pro výklad učiva spjatého s ochranou osobních údajů na internetu žákům, kteří byli zařazeni do kontrolního vzorku (celkem se jedná o 5 tříd, 2 třídy nižšího gymnázia – prima a kvarta a 3 třídy ZŠ – 6. A, 6. B a 9. A). Třídy byly vybrány ze škol, u nichž byl analyzován ŠVP v teoretické části práce. Celková časová dotace na realizaci lekce byla po konzultacích s vedením škol, kde se lekce uskuteční, stanovena na 45 min (1 vyučovací hodina).

10.2 Cíle

Primární cíl navržené vyučovací hodiny je seznámit žáky se zásadami ochrany osobních údajů. Zvolený cíl má zejména ovlivnit postojovou složku žáků. Vzhledem k relativně krátké době, která je výuce věnována a obvykle dlouhodobějšímu působení na postojovou složku žáků, které je potřeba k postupu v taxonomii afektivních cílů, je definovaný cíl optimistický, nicméně považuji ho za reálný. Cíl hodiny zní:

Na konci hodiny žáci ocení zásady ochrany osobních údajů jako užitečné a jejich aplikaci v praxi budou považovat za přínosnou.

Dle Kratwohlovy taxonomie afektivních cílů je možné tento cíl zařadit na 3. stupeň odpovídající oceňování hodnoty, přesněji přesvědčení o hodnotě. [90 s. 284]

Afektivní rovina není jediná, ve které výchovně-vzdělávací proces působí. Dochází také k naplňování kognitivních cílů, výše zmiňovaný afektivní cíl v sobě zahrnuje „aplikaci v praxi“ a právě cíle snažící se dosáhnout alespoň 3. stupně Bloomovy taxonomie kognitivních cílů (aplikace) [90 s. 280–281] jsou nedílnou součástí ukázkové hodiny. Konkrétní znění kognitivních cílů je součástí podrobnějšího výukového plánu (příloha C), v kontextu celé hodiny je ovšem chápeme jako pilíře podpírající cíl konečný – afektivní.

Z hlediska cílů stanovených RVP bychom ukázkovou hodinu zařadili k následující formulaci *„učit žáky aktivně rozvíjet a chránit fyzické, duševní a sociální zdraví a být za ně odpovědný.“*. [62 s. 13] Jedná se o sociální zdraví a právě tak své osobní soukromí můžeme chápat.

10.3 Očekávané výstupy a klíčové kompetence

Jak již bylo uvedeno v teoretické části při rozboru RVP (podkapitola 7.1), nejblíže k očekávanému výstupu, ke kterému směřuje i ukázková hodina je tato formulace: *„chrání data před poškozením, ztrátou a zneužitím,“*. [62 s. 35] Sice se jedná o očekávaný výstup pro 1. stupeň, myslím si však, že učivo ve větší komplexnosti a složitosti je zcela relevantní i pro celý 2. stupeň.

Mezi klíčové kompetence, které jsou ukázkovou hodinou (ale i celou tématikou ochrany osobních údajů) rozvíjeny, patří kompetence občanská, konkrétně potom její aspekt chovat se zodpovědně v situacích, které mohou ohrožovat zdraví – v tomto případě sociální zdraví. [62 s. 13] Vzhledem k povaze Internetu patří mezi klíčové kompetence, které jsou rozvíjeny, i kompetence komunikační a to v této podobě: „*využívá informační a komunikační prostředky a technologie pro kvalitní a účinnou komunikaci s okolním světem.“* [62 s. 15] Nesmíme také zapomenout na kompetenci k řešení problémů, protože každý phishingový útok či pokus o krádež identity je problémovou úlohou, ve které se musí žák správně zorientovat a vyřešit ji. Případné následky znamenají skutečný problém a jejich zmírnění vyžaduje také aktivní přístup stejně jako předcházení takovým situacím.

Není třeba ovšem zde vyjmenované kompetence chápat dogmaticky. Vzhledem k velmi široce pojímaným kompetencím a výstupům vyžaduje jejich vyjmenování pro problematiku ochrany osobních údajů spíše než exaktní přístup fantasii a notnou dávku kreativity. Tento fakt již byl zmíněn v teoretické části v kapitole věnované RVP a tato podkapitola vysvětlující klíčové kompetence a jejich vztah ke konkrétní vyučovací hodině ji jen mírně doplňuje a dovysvětluje fakta uvedená v teoretické části.

10.4 Obecné zásady

Při tvorbě ukázkové hodiny jsem se pokusil stanovit několik obecných zásad, které by měly být při práci se žáky dodrženy, aby hodina byla co možná nejúčinnější a zároveň pro žáky atraktivní. Zde jsou zásady bodově vypsány a vysvětleny:

1) **Příklady a příběhy.** Raději než zdlouhavě opisovat odborné termíny a snažit se je přijatelně vysvětlit, je cennější rizika internetu demonstrovat, ukázat na příběhu. Pojmový aparát jako je kybergrooming nebo sexting není důležitý, klíčové je uvědomění si rizikovosti počínání, které tyto pojmy ve vědeckém světě zastupují. Pokud je to jen trochu možné, je třeba udávat příklady ze života, vyprávět skutečné příběhy, na zjednodušených příkladech vysvětlovat technicky náročnější záležitosti (např. prolomení hesla, HTTPS).

2) **Interaktivita.** Pokud lze žáky do učební aktivity zapojit, pak je třeba tak učinit. Vybízet je k aktivitě, kladení otázek a hledání odpovědí a řešení. Dotazovat se, ujišťovat se, využívat příkladů, které žáci sami uvedou. Interaktivita je použita již u představení lektora a ukázce rozdílu mezi „online světem“ a tím „hmatatelným“. Interaktivně je i vyprávěn příběh či ukázána technika mirroringu, žáci jsou vybídnuti k hledání „háčků“ u phishingu, dále je interaktivity využíváno při práci s hesly. Důraz je kladen i na spontánní interaktivitu během hodiny (dotazy, vzniklé situace, žákovské příklady).
3) **Závažnost.** Na tragických případech ukázat i ty nejhorší možné scénáře, kam až může neopatrné zacházení s osobními údaji vést. Dokázat žákům, že není dobré brát na lehkou váhu nakládání s osobními údaji, a že podobná situace se může týkat i jich.
4) **Zábavnost.** Nebát se využít humoru v prospěch výuky. Adekvátně vybrané a humorné příklady mohou výuku odlehčit a zároveň pomoci k zapamatování.
5) **Vybídnout k přemýšlení.** Apelovat na vlastní rozum, snažit se žáky donutit přemýšlet o situacích reálných i hypotetických. Pokud je to možné, získávat odpovědi od žáků, z jejich hlav.

10.5 Metody

Při výuce jsou využívány zejména metody slovní, konkrétně monologická forma výkladu prokládaná a obohacená atraktivnějšími metodami – vyprávěním příběhů, včetně interaktivního vyprávění příběhu, kdy žáci z nabízených možností odhadují, jakým způsobem se příběh vyvíjel, a do jinak monologické metody tak přináší prvky interaktivity.

Část hodiny má též formu dialogickou, kdy je vyžadováno i zapojení druhé strany, protože snaha udržet 45 min žáky druhého stupně u více méně monologické přednášky, byť o zajímavém tématu, je nevhodným a kontraproduktivním řešením. Pro aktivity spojené s phishingem je využito i dialogu heuristického, kdy sami žáci postupně přicházejí na jednotlivé aspekty podvodných e-mailů, lektor jejich nápady pouze doplňuje a vybízí je k další aktivitě tím, že klade otázky, které přispívají k objasnění dalších podvodných metod. Doplňující výklad využije až jako metodu doplňkovou.

Během části hodiny, kdy si žáci zkouší nástroj pro kontrolu síly hesla, je použitou metodou i mikroinstruktáž, která stojí někde na pomezí mezi metodami slovními a demonstračními.

Přesnější rozepsání metod je uvedeno v přílohách u plánu hodiny. Rozvedení některých zásad, které byly použity při tvorbě výukové hodiny, je již uvedeno výše v rámci obecných zásad a použité metody jsou použity tak, aby těmto zásadám odpovídaly – zejména interaktivita, která má za cíl nabourat jinak ne příliš atraktivní monologický výklad.

Zajímavým prvkem je i zařazení inscenační metody, konkrétně drobného hraní situačních rolí během výuky (žákovi bude nabídnuta výhra v loterii – součást prezentace phishingu, vysvětlení protokolu HTTPS), zde je metoda spíše na straně učitele a má zde spíše doplňkový a ozvláštňující charakter.

Určitě by bylo vhodné použít daleko větší škálu dialogických aktivit, zejména diskuzi. V obecné rovině jsou takové aktivity doporučovány pro realizaci této problematiky ve výuce, nicméně ukázková hodina je časově omezena a relativně pestré spektrum témat má být probráno v krátkém rámci 45 minut, proto je pro lektora transmisivní přístup časově ekonomičtější. Pokud by bylo tématu věnováno více hodin, bylo by vhodnější použít konstruktivistický přístup a tomu odpovídající metody ve větší šíři.

Dělení a definice použitých metod volně parafrázuje kategorizaci dle Kalhouse. [90 s. 307–327]

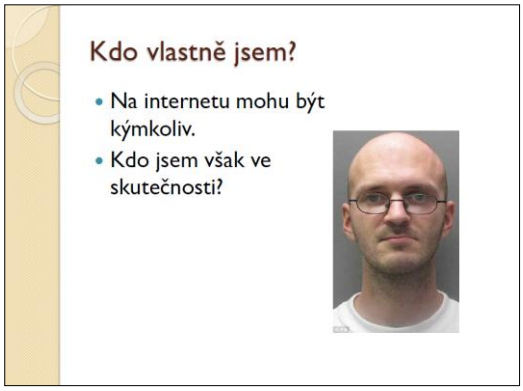
10.6 Organizační forma

Během ukázkové hodiny byla použita organizační forma odpovídající frontální (též hromadné) výuce. [90 s. 295] Individuálně budou žáci postupovat pouze při testování svých hesel nástrojem na kontrolu síly hesla. Zde je naopak žádoucí, aby každý pracoval sám a zachovával diskrétnost. Žáci budou upozorněni, že pokud nechtějí své heslo zkoušet z obavy o jeho vyzrazení, tak nemusí, stačí si nástroj vyzkoušet na libovolném jiném slově či slovech.

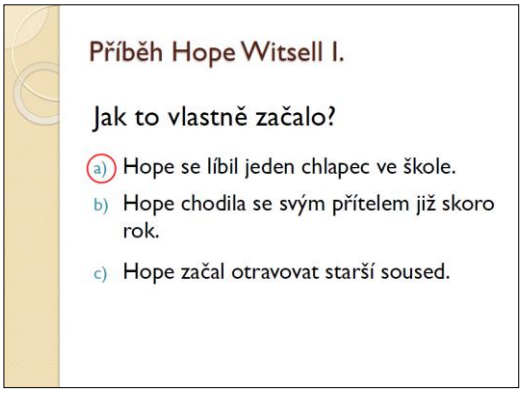
10.7 Pomůcky a materiály

Během ukázkové hodiny slouží k podpoře výuky prezentace ve formátu pdf nebo pptx, která je během výuky promítána, klíčové jsou zejména obrazové materiály, které ilustrují a vysvětlují problematiku. Vzorovou prezentaci lze nalézt na přiloženém CD pod názvem `prezentace_vzor_bp_krahulec.pdf` a obsahuje 36 snímků. Pro ilustraci jsou uvedeny obrázky 10.1 a 10.2.

Dalším využitým nástrojem je měřič síly hesla na stránkách `Passwordmeter.com`, který je žákům představen a mohou si jej také vyzkoušet (pokud mají přístup k počítačům, což není nutná podmínka pro absolvování lekce, nicméně je to vhodné).



Obrázek 10.1: Snímek ze vzorové prezentace s podtitulem „Kdo vlastně jsem“



Obrázek 10.2: Snímek ze vzorové prezentace s podtitulem „Příběh Hope Witsell“

10.8 Vstupní informace

Žáci, pro které je ukázková hodina určena, by měli ovládat základy práce s počítačem, zejména by měli s jistotou ovládat internetový prohlížeč. Další vstupní znalostí je porozumění základním principům autentizace (přihlašování pod uživatelskými jmény a hesly). Dále je nutné, aby žáci rozuměli základům práce s elektronickou poštou a nejlépe ji sami aktivně využívali. Znalost problematiky sociálních sítí je vítaná, nicméně hodina je určena i žákům, kteří nemají účty na takovýchto sítích či je aktivně nevyužívají. Učivo je vyloženo i s ohledem na tyto žáky, aby se i oni seznámili se základy používání sociálních sítí, pokud se s nimi ještě nesetkali.

11 Dotazníkové šetření

11.1 Výzkumný problém

Dotazníkové šetření, které bylo realizováno jako součást této práce, si klade za cíl zjistit, jaké jsou znalosti, dovednosti a postoje o ochraně osobních údajů na internetu ve věkové skupině odpovídající 6. a 9. třídě základních škol. Výzkumný problém je z velké části deskriptivní a snaží se podat ucelený pohled na bezpečnost či nebezpečnost návyků žáků, jejich schopnosti zacházet se svými osobními údaji na síti bezpečně a též se snaží zjistit, zda žáci znají základní pojmy a nástroje související s ochranou osobních údajů a zda jejich znalost dokážou aplikovat.

Cílem výzkumu není jen podat deskriptivní popis, ale obohatit jej o složku relační odpovídající na otázku, zda jsou znalosti, dovednosti a postoje závislé na základních proměnných, z nichž nejdůležitější je věk (ročník), dále potom počet absolvovaných ročníků IKT, pohlaví či typ studované školy a to zejména ve vybraných jevech. Druhou důležitou zkoumanou relací je v tomto výzkumu výuka zásad ochrany osobních údajů (absolvování ukázkové lekce) a její vliv na znalosti, dovednosti a postoje žáků týkajících se dané problematiky.

11.2 Výzkumné metody

Jak již bylo detailně popsáno v teoretické části práce, metodou využitou pro sběr dat byl online dotazník pro žáky výše zmiňovaných věkových kategorií. Dotazník byl realizován pomocí formulářů, které jsou součástí Google Docs, další možné varianty pro online dotazníkové šetření a jeho výhody oproti klasickému „papírovému“ šetření jsou již rozebrány v teoretické části práce v kapitole 9.

11.3 Výzkumný vzorek

Respondenti této práce byli rozděleni do 2 skupin. První skupina čítající 168 respondentů z oslovených základních škol a gymnázií sloužila jen ke zjištění výchozího stavu úrovně znalostí, dovedností a postojů v oblasti ochrany osobních údajů. S touto skupinou se po vyplnění dotazníku již dále nepracovalo. Druhou skupinu tvořil vzorek žáků, kteří nejprve vyplnili dotazník, poté absolvovali jednu vyučovací jednotku (45 min), která se zabývala tématikou ochrany osobních údajů na internetu. Po cca 5 dnech, kdy došlo k uvolnění krátkodobé paměti žáků podle tzv. Ebbinghausovi křivky zapomínání [91] a bylo možno předpokládat, že žáci budou odpovídat zejména na základě trvale zapamatovatelných pojmů, žáci dotazník znovu vyplnili. Tuto skupinu tvořilo celkem 120 žáků, nicméně pouze 88 z nich odpovědělo i na druhé dotazníkové šetření a splnilo tak podmínky pro zahrnutí do kontrolní skupi-

ny. Celkem na dotazník v první vlně odpovědělo 290 respondentů, 2 dotazníky byly vyškrtnuty jako neplatné, soubor tedy čítal 288 respondentů.

Žáci, kteří byli do vzorku zařazeni, chodili do 6. nebo 9. tříd základních škol, nejednalo se tedy o celý druhý stupeň. Byly záměrně vybrány tyto dvě hraniční skupiny, které vymezují nástup na druhý stupeň ZŠ a jeho ukončení. Díky takto definovaným skupinám bylo možné lépe zkoumat předpokládaný progresivní vývoj u znalostí, dovedností a postojů týkající se problematiky ochrany osobních údajů na internetu (viz níže v podkapitole věnované výzkumným hypotézám 11.4).

11.4 Výzkumné hypotézy

Vzhledem k absenci podobně orientovaného výzkumu s odpovídajícím výzkumným vzorkem v naší zemi bylo potřeba stanovit výzkumné hypotézy velmi opatrně a spíše v obecné rovině. Většina prováděných výzkumů u nás i v zahraničí se obvykle orientuje spíše na popisné aspekty prevalence rizikové komunikace, některé jevy (zejména v popisné rovině) sledované v dotazníku jsou srovnatelné s výzkumy, které provádějí Krejčí a Kopecký [8] či byly prováděny ve spolupráci se serverem Safer Internet [29]. Většina otázek použitých v dotazníku je však nová a spíše než k potvrzování hypotéz vycházejících z předešlého pedagogického výzkumu či teorie bude sloužit k detailnějšímu prozkoumání dané problematiky a jako základ pro další podobně orientované práce.

Byly formulovány 2 výzkumné hypotézy, jejichž ověření je vzhledem k dalším aspektům práce (analýza RVP a ŠVP a tvorba výukových materiálů) velmi důležité:

H1:S přibývajícím školním věkem dochází k progresivnímu zlepšování znalostí, dovedností i postojů v problematice ochrany osobních údajů na internetu.

Jinými slovy žáci 9. ročníků mají hlubší znalost zásad ochrany osobních údajů a chrání své osobní údaje lépe než žáci 6. ročníků.

H2:Žáci kontrolní skupiny v dotazníkovém šetření po výuce relevantního učiva prokázali zlepšení úrovně znalostí, dovedností i postojů v problematice ochrany osobních údajů na internetu.

11.5 Předvýzkum

Před samotným uvedením dotazníku do oběhu byl proveden předvýzkum, kde se zjišťovala srozumitelnost otázek pro cílové skupiny a časová náročnost vyplnění celého dotazníku. Předvýzkum byl proveden u skupiny 5 žáků 6. ročníku a 7 žáků 9. ročníku.

Na základě analýzy připomínek a času, který žáci vyplňováním strávili, byla doplněna nápověda k jedné otázce (č. 22), byly přeformulovány některé otázky, kde žáci mohou zaškrtnout více správných odpovědí tak, aby byla tato možnost zřejmá (otázky č. 12, č. 22, č. 23), dále byly provedeny mírné stylistické korekce a zjednodušení některých formulací. Celková doba vyplnění dotazníku se pohybovala od 7 do 12 minut. Pro další účely bylo pracováno s přibližnou délkou vyplňování 10 minut.

11.6 Obsah dotazníku

Dotazník se skládá z celkem 26 otázek, 25 otázek je uzavřených a jedna otázka je polouzavřená (možnost uvést sociální síť, která nebyla uvedena ve výčtu možností).

První část dotazníku má za cíl zjistit základní údaje o respondentovi, které jsou relevantní k popisu dat a k případné identifikaci vztahů. Jedná se o pohlaví, věk, ročník, typ studované školy (ZŠ či nižší gymnázium) a prospěch v předmětu informační a komunikační technologie.

Další část dotazníku se zabývá zjišťováním informací o používání sociálních sítí, sdílení informací na nich, znalosti možností, které sociální sítě nabízejí a postoji ke zveřejňování osobních údajů, část otázek je zde konkrétně mířena na uživatele sociální sítě Facebook.

Ve třetí části je prostor věnován zkušenostmi s krádeží identity a návykům respondenta při práci s hesly či znalosti nástrojů, kterých může při tvorbě hesla a práci s ním využít. Otázky se také věnují klíčovým aspektům nejčastěji používaného hesla, včetně otázek, které pomáhají identifikovat jeho sílu (heslo respondenti ze zřejmých důvodů neuvádějí), podstatnou je zde i diagnostika dovednosti správně vybrat kvalitní heslo.

Poslední část testuje znalost a porozumění klíčovému pojmu HTTPS a také se zaměřuje na respondentovu dovednost rozpoznat phishingovou zprávu.

Celkově je dotazník složen z otázek, které pomáhají jednoznačně diagnostikovat znalosti a dovednosti týkající se ochrany osobních údajů, dále jsou přítomny otázky, které zkoumají postoje respondenta a pomáhají analyzovat, jak bezpečně se uživatel na internetu chová (ve vztahu k osobním údajům). K porozumění datům a zejména vztahům mezi nimi, jsou dále přidruženy otázky, které mohou pomoci identifikovat další doplňující návyky či jevy.

Pro vytvoření profilu, který vypovídá o bezpečnosti a nebezpečnosti práce s osobními údaji na internetu bylo vybráno 9 otázek, které byly bodově ohodnoceny. Bodové hodnocení bylo přidělováno na základě nebezpečnosti návyků, čím vyšší bodové ohodnocení tím nebezpečnější návyk, postoj či odpověď. Metodika bodování odpovědí je součástí příloh a doplňuje celé znění dotazníku, které je uvedeno v přílohách (příloha E).

11.7 Metody zpracování dat

Data získaná z elektronického dotazníku byla exportována do formátu xls a za použití tabulkového procesoru Microsoft Excel byla dále zpracovávána pomocí základních statistických prostředků, které tento program nabízí. Při testování hypotéz bylo dále využito Pearsonova koeficientu korelace (vzorec 11.1) a bodové biseriální korelace (vzorec 11.2). [92]

$$r_p = \frac{\sum(x-\bar{x})(y-\bar{y})}{\sqrt{\sum(x-\bar{x})^2 \cdot \sum(y-\bar{y})^2}} \qquad \text{(Vzorec 11.1)}$$

$$r_{bb} = \frac{\bar{x}_p - \bar{x}_q}{\sigma} \cdot \sqrt{p \cdot q} \qquad \text{(Vzorec 11.2)}$$

11.8 Výsledky a interpretace dotazníkového šetření

11.8.1 Prolomení účtu

Z porovnání provedeného dotazníkového šetření a výzkumu realizovaného Kopeckým a Krejčí v roce 2011 u širší věkové skupiny [8 s. 6], vyplývají některé zajímavé skutečnosti a souvislosti. Za prvé je to prevalence prolomení účtů u respondentů – Kopecký a Krejčí uvádějí téměř 33 % [8 s. 9]. V provedeném dotazníkovém šetření se stalo obětí takového činu pouze 18 % respondentů, dále byla snaha zachytit ještě jemnější nuance. Doplňkového jevu půjčení elektronického účtu další osobě se dopustilo 25 % respondentů dotazníkového šetření, věkové rozdíly přitom nehráli zásadnější roli (v řádech procent). Souhrnně tyto skutečnosti ilustruje tabulka 11.1. Možná diskrepance může být dána širší variabilitou věkové skupiny, menším (tedy méně reprezentativním) počtem respondentů mého výzkumu, nicméně rozdíl je statisticky významný.

	Nebezpečí el. komunikace 2	6. ročníky (toto šetření)	9. ročníky (toto šetření)	Celkem (toto šetření)
Prolomení el. účtu	33 %	20 %	16 %	18 %
Půjčení el. účtu	–	21 %	28 %	25 %

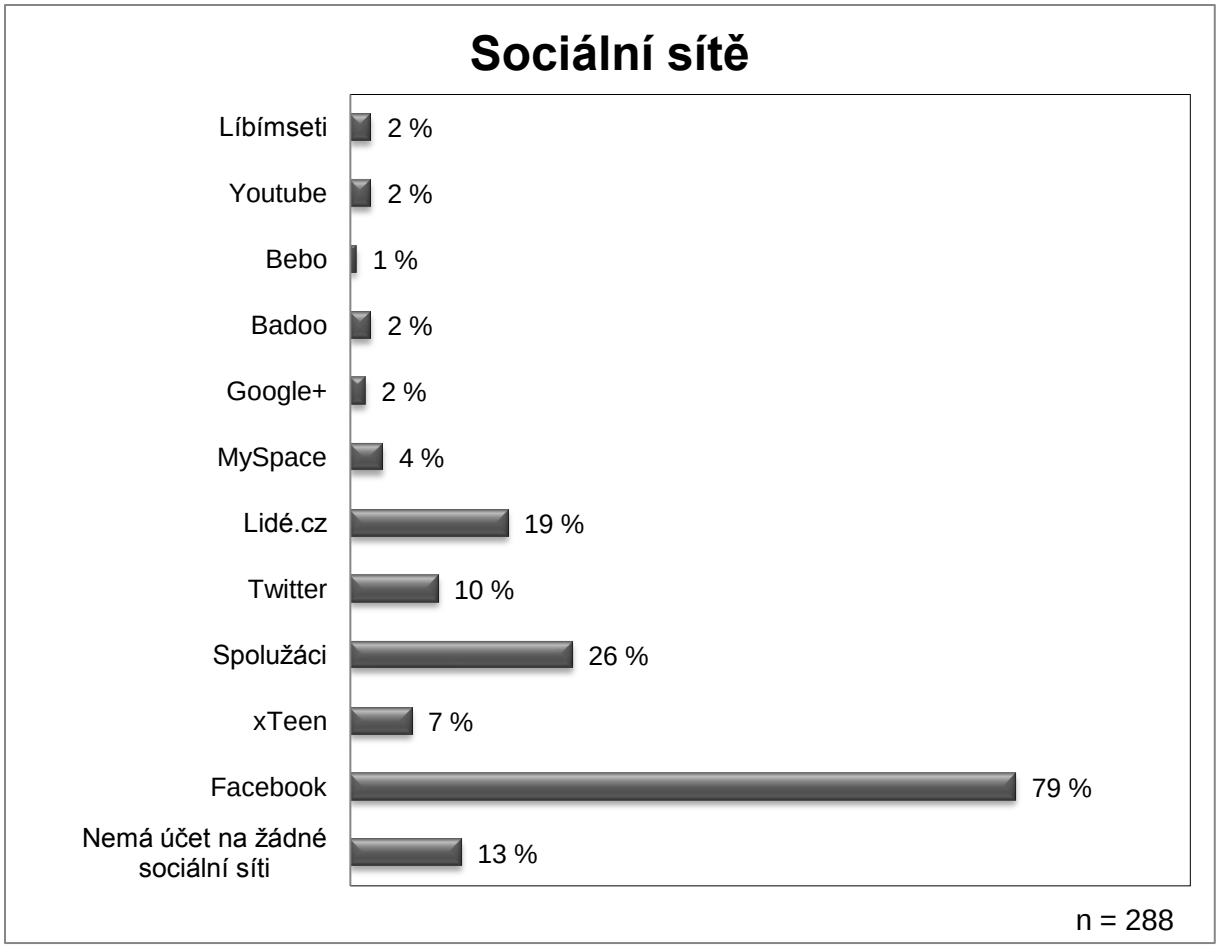
Tabulka 11.1: Prolomení a půjčení účtu – srovnání výsledků výzkumu Kopeckého a Krejčí a tohoto dotazníkového šetření.

11.8.2 Sociální sítě

Pokud porovnáme oblíbenost sociálních sítí v roce 2011 dle Kopeckého a Krejčí a mého výzkumu, je možné zaznamenat několik zajímavých trendů a srovnání, vše je podrobně zaznamenáno v příloze F, klíčový přehled je demonstrován na grafu 11.1. Nejrozšířenější sociální síť Facebook dosáhla v obou výzkumech totožného zastoupení (s odlišností několik setin procenta) s dominantními 79 % uživatelů. Pokud se zaměříme na méně rozšířené sítě,

např. na server Spolužáci.cz, ten zaznamenává v mém šetření velmi citelný pokles obliby uživatelů, který je dle mého dán stále dominantnějším využíváním služeb Facebooku na úkor jiných sociálních sítí a to zejména mezi mladšími respondenty – mezi žáky 6. ročníků využívá tuto službu pouze 12 % žáků, což je proti 50 %, které uvádí Kopecký a Krejčí [8 s. 24] razantní ústup. Dá se předpokládat, že starší uživatelé budou účet stále používat „ze zvyku“, nicméně noví uživatelé sociálních sítí sáhnou spíše po uvedeném Facebooku – i přes věkovou restrikci tam má účet téměř 70 % žáků 6. ročníků. Tomuto jevu se ještě budu věnovat podrobněji níže v podkapitole 11.8.3. Velmi zajímavý zvrat proběhl u seznamky s prvky sociální sítě Líbímseti.cz, jejíž podíl je v mém výzkumu zanedbatelný (2 %), Kopecký a Krejčí ve své zprávě uvádějí více jak 21 %, na tomto poli se totiž objevil nový hráč, který odlákal značnou část mládeže, která dříve využívala tento server, a to portál xTeen.cz, který v uvedeném výzkumu není sledován, nicméně mezi respondenty námi provedeného šetření ho využívá 7 % a to překvapivě více respondentů zejména mezi 6. ročníky, kteří obecně méně využívají služeb sociálních sítí. Za zmínku ještě stojí zastoupení sítě Lidé.cz (19 %), kterou Kopecký a Krejčí nijak nezmiňují. Stabilní postavení si drží též Twitter s 10 % uživatelů, zastoupení ostatních sítí je okrajové.

Mezi mladými tak můžeme do jisté míry hovořit o trendu výrazného přimykání k nejrozšířenější sociální síti (Facebooku), toto postavení nedokázal hlouběji narušit žádný z existujících serverů ani hráči noví (Google+). Jedinou drobnou výjimkou je již zmiňovaný server xTeen.cz, který dle mého těží z cílení na teenagery a nastupuje na místo dříve oblíbeného Líbímseti.cz. Podíl dětí, které mají sociální sítě, se blíží k 90 %, které uvádí i Kopecký a Krejčí [8 s. 23], ti ovšem zahrnují i starší věkové skupiny, u 6. ročníků je typické spíše nižší zastoupení využití sociálních sítí (80 %), 9. ročníky potom uvedenou 90 % hranici mírně přesahují. Drtivá většina mládeže využívá sociálních sítí a je tedy žádoucí tento trend dynamicky zohledňovat při tvorbě obsahů výuky a kurikulárních dokumentů nejen pro ICT ale např. i pro občanskou či mediální výchovu. Ignorovat tento trend by znamenalo přehlížet službu, kterou využívají 4/5 žáků ZŠ.



Graf 11.1: Účty na sociálních sítích u celého vzorku respondentů

11.8.3 Facebookový paradox

Již bylo uvedeno, že sociální síť Facebook je velmi oblíbená také u žáků 6. ročníků, ti ovšem v drtivé většině nesplňují svým věkem podmínky stanovené tímto serverem, tento fakt velmi dobře ilustruje tabulka 11.2 a 11.3.

Věk	Počet žáků celkem	Účet na Facebooku	
11	40	27	68 %
12	81	57	70 %
∑	121	84	69 %

Tabulka 11.2: Žáci nesplňující věkový limit a přesto mající účet na sociální síti Facebook

Věk	Počet žáků celkem	Četlo podmínky na FB	
11	40	17	43 %
12	81	27	33 %
∑	121	44	36 %

Tabulka 11.3: Žáci nesplňující věkový limit soc. sítě Facebook, kteří četli podmínky užívání této sociální sítě

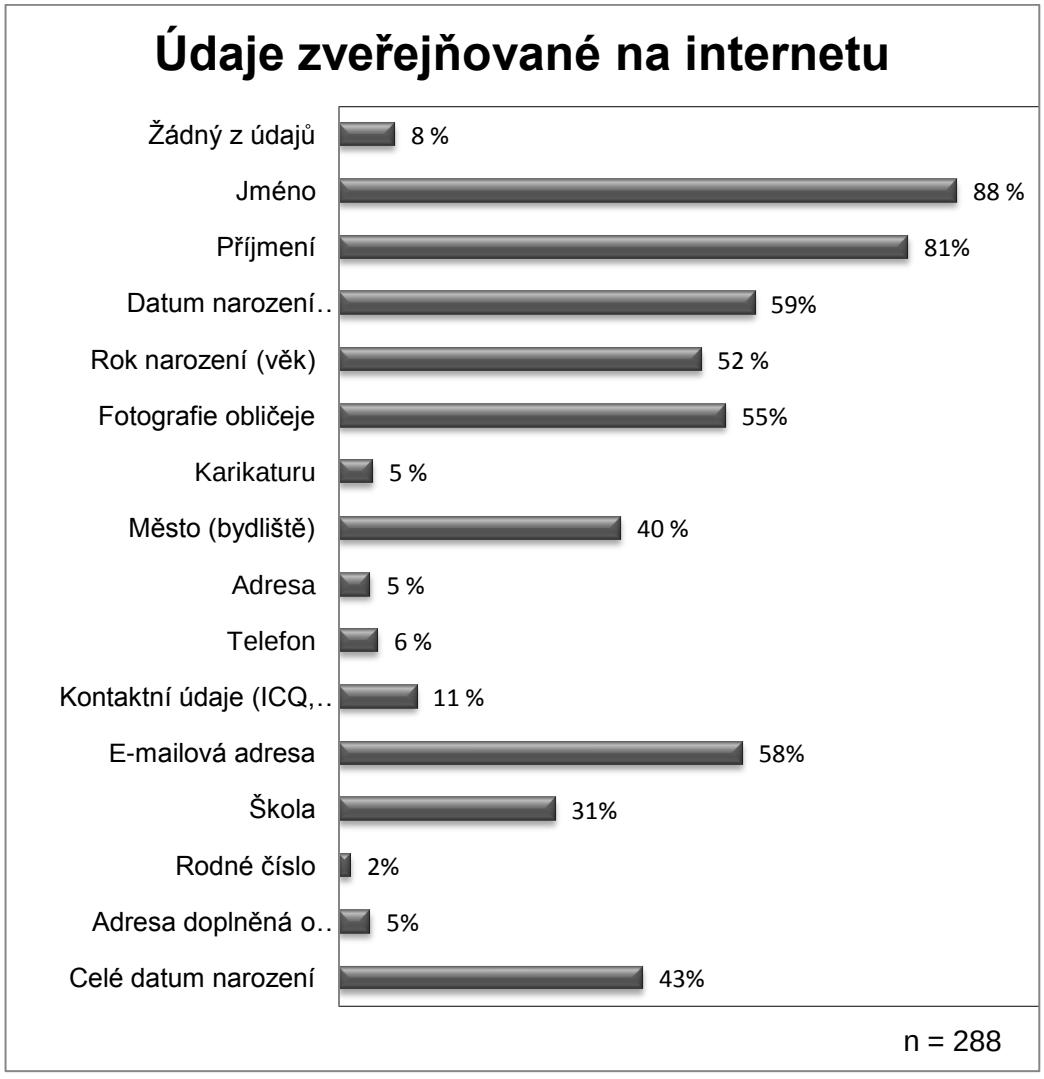
69 % žáků ve věku 11 a 12 let má účet na Facebooku, a to i přesto, že nesplňují jeho podmínky, museli tedy logicky vyplnit jiné datum narození. Pokud se ponoříme hlouběji, zjistíme, že 36 % uživatelů Facebooku, kteří nesplňují věkovou hranici, uvedlo, že četlo podmínky užívání, tito žáci tedy museli podmínky porušovat záměrně. Ostatní uživatelé na tuto restrikci pravděpodobně narazili při zadávání věku či o ní vůbec nevědí (zde se již pohybujeme na poli spekulací). Zajímavým paradoxem je, že služby sociálních sítí využívají ve velké míře i uživatelé, kterým sociální síť není určena. V tomto ohledu je server bezradný. Je velmi jednoduché uvést fiktivní datum narození, které splní podmínky a možnost kontroly je nulová. Obsah, který mohou děti prohlížet je potom často nevhodný vzhledem k jejich věku. Stejně tak se děti stávají mladými a nezkušenými oběťmi predátorů, stalkerů či lovců osobních údajů. Dobrovolně tak vstupují na hřiště, kam mají vstup zakázán a hrozí zde potenciální rizika. Snaha tomu zabránit je bezzubá a snadno se dá obejít. Jednoduché řešení takového problému ovšem neexistuje, i kdyby podmínky věku byly ještě více zvýrazněné, děti často dobrovolně tuto mez překračují a sankcí jim může být pouze smazání účtu. V tomto ohledu je žádoucí začít seznamovat děti s principy ochrany osobních údajů na internetu již v raném věku a nespoléhat se na to, že se jich to „ještě netýká“, výzkum ukazuje pravý opak.

11.8.4 Zveřejňování osobních údajů na internetu

Pokud zveřejňování osobních údajů zjištěných z tohoto výzkumu porovnáme s údaji uvedenými ve výzkumné zprávě Kopeckého a Krejčí z roku 2011 [8 s. 19] je patrné, že respondenti tohoto výzkumu umisťují na internet údaje osobní povahy, které mohou být viděny jako méně nebezpečné (jméno a příjmení, fotografii) častěji, než jak to naznačuje starší výzkum – toto souvisí dle mého zejména s podstatou služby sociálních sítí a zejména Facebooku, který spíše pracuje s dostupnějšími údaji (fotografie, jméno, příjmení, věk, narozeniny), které jsou hlavními údaji poskytovanými na této síti – na základě těchto údajů, můžeme mluvit o poskytování osobních údajů dle zákona, protože poskytnuté údaje jednoznačně identifikují jedince. Jedná se však o nárůst, který není dramatický a pohybuje se do 10 %.

Druhým zjištěním je podstatně nižší poskytování údajů, které vedou k přímé vystopovatelnosti oběti v reálném světě (adresa) či navázání komunikačního kanálu s obětí (IM, e-mail, telefonní číslo). Zatímco e-mail poskytuje jen zanedbatelně menší množství respondentů, kontaktní údaje na IM, adresu či telefonní číslo poskytuje daleko menší množství respondentů, pro porovnání – telefonní číslo 6/23 %, adresa 5/16 %, IM a VoIP (ICQ, Skype) 11/30 %. Tento trend můžeme vyložit jinou věkovou základnou (jak ukazují tabulky F.48 a F.49 v příloze F) mladší respondenti zveřejňují v průměru méně osobních informací než

starší respondenti, tento rozdíl není však tak dramatický). Další možnost spatřuji v přesunu komunikačních kanálů z výše zmiňovaných platforem právě na Facebook, který zahrnuje systém zasílání zpráv i chatu a žáci tedy nemají tendenci další doplňkové údaje poskytovat, třetí možností je rozšíření povědomí o nebezpečnosti poskytování osobních údajů a v tomto ohledu obezřetnější chování, tomuto předpokladu by odpovídaly i odpovědi o nebezpečnosti zveřejňovaných údajů, kde telefonní číslo označilo za nebezpečné 78 % a adresu více jak 85 %. Velmi zajímavé budou v tomto ohledu nové výsledky centra Prvok (studie připravovaná Kopeckým a Krejčí pro tento rok) a budou moci některé z těchto trendů potvrdit či vyvrátit. Zatímco první trend častého zveřejňování jména, příjmení, data narození a fotografie můžeme vnímat za znepokojivý, trend druhý, který vede spíše k zatajování dalších osobních údajů je dobrou vyhlídkou, dovoluji si ovšem upozornit, že dotazníkové šetření se může do jisté míry lišit od skutečné praxe a ke skutečnému vhledu by bylo potřeba rozsáhlejší případové studie, která zatím v našem prostředí zcela chybí.



Graf 11.2: Údaje zveřejňované na internetu

11.8.5 Ověření hypotézy č. 1

H1: Žáci 9. ročníků mají hlubší znalost zásad ochrany osobních údajů a chrání své osobní údaje lépe než žáci 6. ročníků.

K ověření této hypotézy bylo využito 9 otázek, které byly bodovány v závislosti na bezpečnosti či nebezpečnosti postojů žáků, či vybraných odpovědí, které ověřovaly dovednosti a znalosti spojené s touto problematikou. Výsledky pro každý ročník zvlášť zachycují tabulky 11.4 a 11.5 a graf 11.3, další dílčí odpovědi a jejich zpracování je zaznamenáno v příloze F.

Trestné body	Četnost (n_i)	Relativní četnost (f_i)
0	2	2 %
1	8	6 %
2	16	13 %
3	18	14 %
4	19	15 %
5	16	13 %
6	11	9 %
7	15	12 %
8	7	6 %
9	7	6 %
10	3	2 %
11	1	1 %
12	3	2 %

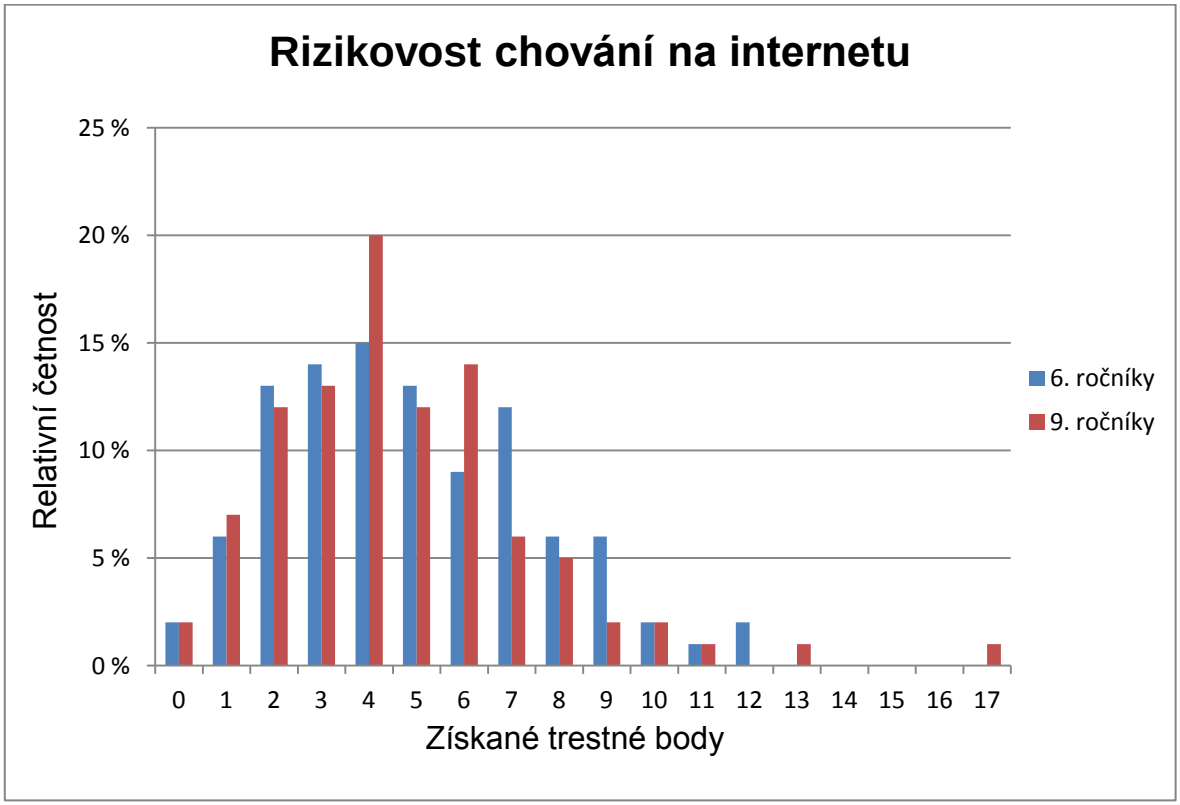
Aritmetický průměr bodového skóru ($\bar{x}$)	4,90 b.

Tabulka 11.4: Rozložení bodového skóru u žáků 6. ročníků

Trestné body	Četnost (n_i)	Relativní četnost (f_i)
0	4	2 %
1	11	7 %
2	20	12 %
3	21	13 %
4	33	20 %
5	20	12 %
6	23	14 %
7	10	6 %
8	8	5 %
9	3	2 %
10	4	2 %
11	2	1 %
12	0	0 %
13	2	1 %
14	0	0 %
15	0	0 %
16	0	0 %
17	1	1 %

Aritmetický průměr bodového skóru ($\bar{x}$)	4,63 b.

Tabulka 11.5: Rozložení bodového skóru u žáků 9. ročníků



Graf 11.3: Rozložení získaných trestných bodů u 6. a 9. ročníků

Pro ověření závislosti ročníku a bodového skóru bylo využito výpočtu Pearsonova koeficientu korelace (vzorec 11.1) a koeficientu bodové biseriální korelace (vzorec 11.2). Oba vzorce jsou uvedené v kapitole 11.7.

V obou případech byla zjištěna velmi slabá závislost bodového skóru na ročníku. V případě Pearsonova koeficientu korelace se jednalo o $\mathbf{r_p = 0,05}$ a v případě biseriální korelace byl výsledek při zvolené úrovni přesnosti totožný $\mathbf{r_{bb} = 0,05}$. Velmi malý rozdíl je patrný i při letmém pohledu na průměrné skóry obou skupin $\mathbf{\bar{x}_9 = 4,63}$ (9. ročníky, y = 0), $\mathbf{\bar{x}_6 = 4,90}$ (6. ročníky, y = 1).

Hypotéza č. 1 je tedy statisticky neprůkazná. Zatímco v úlohách zaměřených na dovednosti a znalosti je patrný lepší bodový výsledek žáků 9. ročníků (ne však zásadní) – otázky č. 24, 25, 26, výsledky odrážející návyky týkající se zveřejňování údajů osobní podstaty či návyků spojených s kvalitou a nakládáním se svým heslem jsou žáci 6. ročníků srovnatelní s žáky 9. ročníků či dokonce mírně lepší – otázky č. 22, 23 a zejména 13.

Pokud bychom zkoumali Pearsonův koeficient korelace bodového výsledku v závislosti na typu školy, počtu absolvovaných ročníků ICT či pohlaví, jak ukazuje tabulka 11.5, zjistíme, že jiné proměnné vykazují výraznější stupeň závislosti než zmiňovaný ročník školy. Z výsledků vyplývá, že chlapci dosahovali lepších výsledků než dívky (méně trestných bodů u chlapců) a nižší gymnázia si vedla lépe než ZŠ (výraznější rozdíl), co je ovšem zarážející je zhoršující se bodový skór (více trestných bodů) s více absolvovanými ročníky ICT, sice vychází velmi slabá závislost, nicméně výsledek je to alarmující a zcela popírající fakt, že hodiny ICT by měly rozvíjet znalosti, dovednosti a postoje žáků v problematice ochrany osobních údajů na internetu, a ačkoliv nebyl tento jev přímým předmětem výzkumu, je třeba na něj upozornit a bylo by vhodné jej ještě dále verifikovat dalším a detailnějším výzkumem s větší skupinou respondentů. Jako jedno z možných vysvětlení se nabízí tzv. „profesionální slepota“ uživatelů, jinými slovy si uživatelé na komunikaci na internetu zvykli a jejich ostražitost polevila.

	Nižší gymnázia (0) ZŠ (1)	**Chlapci (0)** děvčata (1)	Absolvované ročníky ICT (**0**–5)	**9. ročník (0)** 6. Ročník (1)
Pearsonův koeficient korelace (r_p)	0,31	0,18	0,14	0,05

Tabulka 11.6: Koeficient korelace nezávislých proměnných (škola, pohlaví, absolvované ročníky ICT, ročník) a závislé proměnné (trestné body). Čísla v závorkách udávají hodnotu y, která byla prvkům přiřazena, nebylo-li to jinak zřejmé z podstaty dat (počet absolvovaných ročníků ICT).

11.8.6 Ověření hypotézy č. 2

H2: Žáci kontrolní skupiny v dotazníkovém šetření po výuce relevantního učiva prokázali zlepšení úrovně znalostí, dovedností i postojů v problematice ochrany osobních údajů na internetu.

Kontrolní skupinu pro ověřování této hypotézy tvořilo původně 120 žáků (skupina označená hodnotou 1 pro výpočet Pearsonova koeficientu korelace) – ti absolvovali vzorovou a hodinu a poté měli v rozmezí 3–7 dní opětovně vyplnit dotazník. Dotazník znovu vyplnilo pouze 88 žáků (hodnota 0) v důsledku nezájmu či nemožnosti kontroly ze strany vyučujících v jedné či dvou třídách. Výsledky těchto 88 žáků byly porovnávány s jejich původními výsledky a bylo zjišťováno, do jaké míry měla vzorová hodina vliv na úpravu postojů, zlepšení znalostí a dovedností v problematice osobních údajů. K výpočtu bodů bylo tentokrát použito pouze 7 otázek (č. 13, 18, 22, 23, 24, 25, 26), kde bylo možné, aby došlo ke změně v odpovědích žáků. K výpočtu závislosti bylo opět použito Pearsonova koeficientu korelace a biseriální korelace a opět s totožnými výsledky $\mathbf{r_{bb} = 0{,}32}$. a $\mathbf{r_p = 0{,}32}$ (ve prospěch výsledků kontrolní skupiny po absolvování vzorové hodiny). Výrazný posun byl vidět již při porovnání průměrného počtu trestných bodů před a po vzorové hodině, došlo ke zlepšení o **1,38 b.** V tomto ohledu již můžeme mluvit o statisticky významném rozdílu, závislost Pearsonova koeficientu korelace spadá do kategorie nízké závislosti, nicméně výsledek je nejsilnější závislostí, která byla zachycena.

Posun se odehrál zejména v kognitivní složce. Abychom mohli ještě lépe zmapovat vliv vzorové hodiny, bylo by nutné měřit výsledky ještě jednou s delším časovým odstupem, kdy by se pravděpodobně vlivem zapomínání snížil vliv kognitivní složky a naopak by se mohl silněji promítnout vliv změny postojů a návyků (úprava profilů, volba nového hesla, změna chování ve vztahu k osobním údajům).

Závěrem můžeme hypotézu považovat za pravdivou a statisticky prokázanou, nicméně skutečný účinek vzorové hodiny by bylo třeba ještě dále dlouhodobě zkoumat pro získání lepší a přesnější představy.

11.8.7 Překvapivá fakta a zamyšlení nad výsledky

Výsledky se nakonec ukázaly pozitivnější, než byl původní předpoklad, např. žáci zveřejňují daleko méně informací vedoucí k jejich kontaktování a vystopování, než byl původní předpoklad na základě analyzovaných studií. Více než 80 % žáků dokáže vybrat nejbezpečnější heslo z možných a téměř 88 % respondentů rozpoznalo phishingový mail. Vlastní hesla mělo mnoho žáků na velice dobré či alespoň dostatečné úrovni, celkem 85 % žáků se pohy-

bovalo v rozmezí 0–2 trestné body a dobré znalosti a zájem o problematiku byl patrný i během ukázkových hodin u velké části žáků.

U této problematiky je důležité zaměřit se spíše na výsledky všech než na porovnávání průměrných hodnot. Phishing, prolomení účtu, podvodné skupiny, sběr osobních údajů pro marketingové účely či šíření spamu nejsou jevy, které by uspěly u širokého spektra lidí, naopak mají úspěšnost velmi malou. Jedná se však o jevy, které jsou masivně distribuované, a proto jim v podstatě stačí získat či nachytat velmi malé procento lidí, a i tak získají v absolutních číslech nezanedbatelný počet obětí, proto by mělo být cílem vzdělat všechny žáky a působit na postoje každého jedince, protože těch několik málo jednotek procent, které sítem takzvaně neprojdou – odpověděli by na phishingový e-mail (3,5 %) či by si zvolili za nejbezpečnější heslo kombinaci 12345678 (4 %). Stejně jako je žádoucí, aby každý byl gramotný, protože číst a psát bude muset při každé příležitosti, mělo by být cílem formovat u všech žáků takové postoje a učit je takovým dovednostem a znalostem, které je co nejlépe připraví na stále se rozpínající online svět, jeho možnosti, ale také jeho nástrahy.

Instituce, která by měla prostřednictvím hodin ICT žáky v tomto směru rozvíjet, je škola, nicméně z výsledků uvedených v podkapitole 11.8.6 vyplývá, že počet absolvovaných ročníků ICT pozitivně neovlivňuje znalosti, dovednosti a postoje žáků k ochraně osobních údajů. Společně s nepotvrzením hypotézy č. 1, dostáváme jasné signály, že se této tématice nevěnuje pozornost nebo se nedaří u žáků vybudovat žádoucí postoje, dovednosti a znalosti v oblasti ochrany osobních údajů. Ať se jedná o kterýkoliv ze jmenovaných faktorů, vidím jako velmi důležité se snažit tuto realitu změnit.

12 Úprava metodických materiálů

12.1 Reflexe vyučovacích hodin

V rámci práce bylo odučeno celkem 6 vyučovacích jednotek po 45 minutách. Zde jsou shrnuty jevy a postřehy, které by stálo za to vzít v potaz při znovupoužití materiálů či při snahách tématiku celistvěji zahrnout do výuky:

1) Problematika by si jednoznačně zasloužila větší časový rámec, časově se podařilo hodiny naplnit a nepřetahovat, nicméně prostor pro aktivity a dotazy žáků by bylo vhodné rozšířit.
2) Vyprávění příběhů bylo pro žáky atraktivní, pokud bylo navíc při aktivitách požadováno jejich zapojení, setkalo se to vždy s úspěchem.
3) Doprovodnou prezentaci bylo vhodnější použít v pdf s možností zvětšit některé detaily v případě potřeby.
4) Vlastní aktivity žáků s nástrojem pro ověřování síly hesla na počítačích měly úspěch a také velmi názorně pomohly žákům utvořit si názor na kvalitu jimi používaného hesla či hesla kandidátního. Pokud by bylo více času, stálo by za to ukázat i manažery hesel či jednoduchý útok pomocí programu pro zjišťování zapomenutých hesel.
5) Žáci měli velké množství dotazů, byli ochotni při jejich zodpovídání přijít i o část přestávky, stálo by za to dát větší prostor pro dotazy, diskuzi, ale i další příběhy žáků, což by byl jev velmi cenný.

12.2 Úprava vzorové vyučovací jednotky

Na základě reflexe a výsledků výzkumu by mohlo dojít k rozšíření repertoáru aktivit spojeného s problematikou. Bylo by dobré přenést těžiště hodiny na žáky, vytvořit z nich průvodce či referující, zde jsou některé konkrétní nápady nastíněny (detailně jsou rozpracovány v přílohách), mají sloužit zejména jako inspirace pro tvorbu podobně zaměřených hodin.

1) Rozšíření časového rámce minimálně na 2 vyučovací hodiny, nově získaný čas by mohl být využit k dalším aktivitám či k diskusi a disponibilně čas využít u již plánovaných aktivit k rozšíření o další příklady.
2) Úvod do tématu by mohl být pojat formou brainstormingu okolo centrálního pojmu **ochrana osobních údajů na internetu / osobní údaje na internetu**, pokud by byla hodina zařazena v rámci širšího celku, mohlo by jít i o **nebezpečí na internetu**.
3) Zařadit do hodiny představení a instruktáž nějakého manažeru hesel (vhodné ho i nainstalovat na školní počítače, aby si práci s ním mohli žáci vyzkoušet).

4) Zařadit do hodiny diskuzi o sociálních sítích, konkrétně Facebooku, doplnit ji o interaktivní provedení po Facebooku, ideálně do role průvodce pasovat nějakého žáka, možnost zadat předem k připravení některému z žáků. Diskutovat o výhodách a nevýhodách, upozornit na některá zajímavá fakta (věkové omezení, licenční podmínky) a funkce (pokud o nich nebude řeč).
5) Za domácí úkol je možné žákům zadat, aby našli vlastní phishingový či jiný podezřelý e-mail (nejlépe z vlastní schránky) a nechat je ho rozebrat či interpretovat. Tuto aktivitu zadat na další hodinu, poté, co již budou vědět, co to phishing je.

13 Doporučení vyplývající z výzkumu

13.1 Obecná doporučení na úrovni kurikulárních dokumentů

Školy by do svých ŠVP měly v rámci informačních a komunikačních technologií kromě práce s textovými editory a tabulkovými procesory také zahrnout působení na úrovni afektivních cílů a pomoci žákům vytvářet si bezpečné návyky na síti, velké množství dětí používá sociální sítě a to již od raného věku, bylo by tedy vhodné zařadit tuto problematiku již na 1. stupni. Znalosti a dovednosti spojené s touto problematikou by bylo vhodné postupně rozvíjet po celý druhý stupeň přiměřeně věku i trendům, které postupně děti zasahují a s ohledem na aplikace, které žáci využívají.

Je samozřejmě možné tuto problematiku zařadit i mimo informační a komunikační technologie, např. v rámci mediální či občanské výchovy, chybou by ovšem bylo tuto problematiku zcela opomíjet a doufat, že se o náležitou osvětu postarají rodiče. V současné době se nacházíme v situaci, kdy je velmi patrný rozdíl mezi digitální generací a tou, která vyrůstala nezasažena Internetem a do značné míry i počítači, nemůžeme tedy počítat s tím, že rodiče své ratolesti poučí, když sami často s moderními technologiemi zápasí. V budoucnosti můžeme očekávat logicky zlepšení, nicméně škola by v tomto procesu měla hrát roli, které se ovšem spíše vyhýbá a soustřeďuje se spíše na jiné učivo v rámci ICT.

Pokud budeme vycházet z dotazníkového šetření, čtvrtina žáků 6. tříd (24 %) doposud „unikala“ předmětu informačním a komunikačním technologiím, ačkoliv RVP předepisuje hodinu ICT již na prvním stupni. Toto svědčí o jistém rozporu, jehož příčiny si netroufám bez znalosti stavu hlouběji analyzovat, nicméně obecně vnímám nedostatek hodin věnovaných ICT jako problém, někde jsou na tuto složku sice využívány hodiny disponibilní, ale celkově je cítit, že zatímco výukový obsah pro tyto hodiny by byl, schází mu spíše prostor, na kterém by mohl být realizován. V tomto ohledu si myslím, že české školství nereaguje dostatečně dynamicky na pronikání ICT do všech složek života společnosti a už vůbec ne na aspekty a trendy, které přináší, třeba právě na masivní rozšíření sociálních sítí.

13.2 Doporučení pro realizaci problematiky v hodinách ICT

V tomto ohledu bych chtěl opět akcentovat problematiku zabezpečování účtů a kritického zvažování obsahu na internetu. Již jsem výše nastínil, že nepovažuji výsledky žáků za špatné, nicméně právě tato problematika, více než jakákoliv jiná, vyžaduje, aby jí byly učeny všechny děti, a aby ji také dokázaly všechny děti ovládnout, i zanedbatelné procento špatně zabezpečených účtů či klientů bank, kteří se nechají snadno nachytat na podvodné zprávy,

představuje velké riziko. Apeluji tedy na učitele, pokud se budou věnovat této problematice, aby nenechávali děti pozadu.

Podíváme-li se na problematiku z odlišné perspektivy, tím, že učitelé ICT nebudou zásady dětem vštěpovat a vyhodnocovat společně rizika sdělování údajů, šíření fotografií, vytvářejí tak do budoucna prostor pro zásadní problém. Dnes na internetu sdílí každý téměř cokoliv, Internet je doslova zahlcen obsahem tvořeným uživateli a je pravděpodobné, že mezi takovým obsahem jsou umístněny i informace a údaje, které by si uživatelé přáli, aby proti nim nikdo nepoužil. Pokud dovedeme vše až do absurdna, každý zaměstnavatel si bude moci velmi detailně proklepnout svého potenciálního zaměstnance (dnes praxe často běžná) a také zde budou informace pro stalkery, útočníky, kteří se budou snažit protivníky zdiskreditovat či vydírat. Právě nezodpovědným chováním si děti mohou na takový problém, jehož důsledky se dlouhé roky neprojeví, zadělávat již nyní. Učitel by měl nutit děti k zamyšlení nad tímto problémem, a ač je diskuze metodou v ICT spíše nevídanou, měla by mít své místo i zde.

Pokud se podíváme ryze pragmaticky na to, co by stálo za to být zařazeno v hodinách ICT (a bylo již zmíněno v praktické části této práce), bude to zejména seznámení dětí s příběhy, které prožili jiní (formou vyhledávání informací dětmi či prostým vyprávěním učitele), určitě by děti měly přidat své příběhy, protože pokud skutečně pocítí, že se jich takové věci týkají (krádež účtu či identity) snáze přijmou zásady ochrany za své. Pro demonstraci síly hesel, šifrovaných protokolů, phishingových zpráv a obecně ochrany osobních údajů existuje velké množství materiálů na internetu (mnoho z nich jsem zmiňoval v teoretické části práce) a učitel má na výběr, které žákům představí.

Zcela konkrétně doporučuji, pokud je to v silách správce, využít služeb APWG a uvést do praxe jejich „přistávací stránku“ či vytvořit vlastní, registrovat a automaticky přesměrovávat podvodné stránky, na které by žáci mohli narazit.

Kromě výuky ovládání klasických programů (jakou jsou např. MS Word, Excel, Power Point či grafický editor) by mohlo být dětem představeno i několik jiných programů a aplikací, které souvisí s hesly (správci, nástroje kontroly síly hesla, nástroje pro prolamování hesla) a s tím i spojené postupy heslování archivů.

Pokud by učitel chtěl vzbudit v žácích zájem o šifrování, jejich princip se dá velmi jednoduše demonstrovat na jednoduchých šifrách (Caesarova šifra) a výuka prostřednictvím šifrovačky může být velmi atraktivní a zároveň může žákům přiblížit princip zabezpečení dat.

Další zajímavou aktivitou zařaditelnou například v rámci dovedností vyhledávání na internetu, může být i vyhledávání informací o sobě, což může dětem demonstrovat, to, jak si je někdo může „vygooglovat“ a co má šanci se dozvědět.

Pokud se blíže podíváme na sociální sítě, učitel by se jim neměl vyhýbat jako případnému tabu, ale měl by žáky nechat předvést, jak se na nich pohybují, co všechno na nich umí či znají, a sám by měl hrát roli jakéhosi průvodce, který může dětem ukazovat některé skryté věci a poukazovat na případná rizika. Nevidím nic špatného na tom, když si společně s učitelem zkusí vytvořit například identitu reprezentující jejich třídu či školu a vhodně ji naplní obsahem, na takovém příkladu se dají dobře demonstrovat kromě výhod i rizika sociálních sítí.

Pokud bychom se od roviny konkrétních příkladů odklonili, dále bych výrazně zdůraznil nutnost propojovat obsahy v rámci mezipředmětových vztahů, jak již bylo několikrát zmíněno, ochrana osobních údajů na internetu nemusí být omezena jen na ICT a velmi dobře by se některé méně technické aspekty uplatnily i v jiných hodinách, např. v občanské výchově, pokud by se podařilo vyučujícím těchto předmětů obsahy propojit, mohlo by to být přínosem i pro žáky.

Poslední doporučení bych směřoval k tomu, že problematiku bezpečnosti na internetu nelze jednorázově odbít hodinou či jednou přednáškou, pokud má být skutečně ovlivněna postojová složka žáků, případně mají-li být znalosti hluboko zakořeněné, je třeba se problematiky dotýkat z různých stran a přistupovat k ní opakovaně, klíčové je rozvíjet tyto složky u všech žáků bez rozdílu a to je úkol jistě velmi náročný.

Závěr

Nemá smysl vytvářet katastrofický obraz „zlého“ Internetu či online světa, který kazí děti, ty jsou v něm zcela bezbranné a vydané napospas nejrůznějším nebezpečím od pedofilů, predátorů, stalkerů až po hackery. Průměrný žák naopak dosáhl v šetření slušných výsledků a katastrofické scénáře, při kterých žáci snadno podlehnou jakékoliv manipulaci (třeba ve formě phishingových zpráv), se tedy nepotvrdily. Žáci si uvědomují rizika poskytování osobních údajů na internetu. Takový obrázek nám alespoň dává provedené dotazníkové šetření.

Dnešní mládež se pohybuje v online světě a je jí daleko více vlastní než generacím starším a stává se často domovem pro druhý život dětí. Tuto skutečnost by měly reflektovat i obsahy vzdělávání a konkrétně jednotliví vyučující a tvůrci ŠVP napříč předměty, to se ovšem často neděje, jak jinak si vysvětlit stagnující úroveň znalostí, dovedností a postojů v této problematice u žáků? Česká škola téma osobních údajů nechává spíše stranou a doufá, že si s tím poradí výchova v rodině, stejně jako je snaha zavádět do škol sexuální výchovu, protože ne v každé rodině se dostane toto téma na pořad dne, analogicky by se mělo přistupovat k ochraně osobních údajů, nechávat žáky nějak se s tím „poprat“ a případně je nechat se spálit, ať se naučí, je krátkozraké a nebezpečné. Jedna chyba může (samozřejmě nemusí) způsobit následky, které se budou i opakovaně vracet po celý život.

Bylo již uvedeno, že průměrný žák dosahuje slušných výsledků. Z hlediska ohrožení je však zajímavá ta část žáků, která nemá dostatečně kvalitní znalosti, dovednosti či postoje této problematiky a je tedy tou nejrizikovější skupinou. Dobrým výsledkem by byla co nejmenší variační šíře, kdy žáci sice nemají znalosti dokonalé (ty se dají dále zlepšovat), ale žádný z nich není snadnou kořistí. Takový úspěch je možné zaznamenat u kontrolní skupiny – jinými slovy, výukou takových met lze docílit. Realita mimo kontrolní skupinu je ovšem odlišná a díky masové distribuci třeba právě podvodných zpráv to útočníkům bohatě stačí. Je zvykem tvořit akční programy „žádné dítě pozadu“, zde je takové heslo přeci jen o trochu více než jen prázdnou frází. Kompetentní využívání osobních údajů a práci s nimi bychom měli považovat za základní dovednost žáka a občana, pokud budu poněkud přehánět, můžu ji i přirovnat k důležitosti dovednosti číst a psát.

Současně je třeba připomenout, že pokud děti publikují své údaje osobní i citlivé povahy na internet, a nemusí to být jen jméno a adresa, ale i fotografie, názory, atp., je možné, že tyto údaje jednou, v tu nejméně vhodnou chvíli, někdo najde a použije proti nim (třeba za 10 let) – digitální stopa, totiž nemizí. Jedna trapná fotka či hloupé zveřejnění rodného čísla nebo nějakého ožehavého komentáře se časem na internetu „vsákne“, ale může se objevit ně-

kde jinde a v málo pravděpodobný čas. Zanecháváme po sobě ve světě online velké množství stop, blížíme se tedy ke společnosti, kde se na každého „něco najde“ a na každého se „něco zajímavého ví“. Budou dnešní děti (a já s nimi) mít strach při každém pracovním pohovoru nebo práci ve veřejné funkci, že se někde „něco objeví“?

Lze položit otázku, která ukazuje další možný směr výzkumu v této oblasti. Je skutečnost vyplývající z dotazníků opravdu věrohodná nebo je jen hrou respondentů? Vhled by nám jistě pomohla získat rozsáhlá případová studie, na které bych chtěl časem pracovat. Trávím mezi dětmi, jejich profily i zveřejňovanými údaji nezanedbatelnou část svého času a myslím si, že realita je více znepokojující než vypadá z výsledků této práce, to je ovšem pouze osobní odhad založený na zkušenostech, prostor pro potvrzení či vyvrácení takového tvrzení bych velmi rád v budoucnu využil.

Použité zdroje

[1] Zákon č. 101/2000 Sb., o ochranně osobních údajů (účinné znění). In *Sbírka zákonů České republiky* [online]. 2012 [vid. 30. 3. 2012]. Dostupné z: http://www.uoou.cz/uoou.aspx?menu=4&submenu=5&loc=20

[2] *Zákony týkající se práce s informacemi + Etická pravidla v prostředí internetu* [online]. 24. 9. 2007 [vid. 1. 3. 2012]. Dostupné z: http://www.fme.vutbr.cz/studium/zavprace/etika/kapitola_8_a.pdf

[3] DOLEČEK, M. Ochrana osobních údajů - zpracování osobních údajů. In: *BusinessInfo.cz* [online]. 16. 9. 2009 [vid. 3. 3. 2012]. Dostupné z: http://www.businessinfo.cz/cz/clanek/orientace-v-pravnich-ukonech/ochrana-osobnich-udaju-zpracovani-opu/1000818/51145/#b7

[4] DOČEKAL, D. Ochrana osobních údajů - zpracování osobních údajů. In: *Lupa.cz* [online]. 23. 1. 2008 [vid. 3. 3. 2012]. Dostupné z: http://www.lupa.cz/clanky/podle-eu-je-ip-adresa-osobnim-udajem/

[5] *COPPA - Children's Online Privacy Protection Act* [online]. Aktualizace 14. 3. 2012 [vid. 14. 3. 2012]. Dostupné z: http://www.coppa.org/comply.htm

[6] FACEBOOK. Prohlášení o právech a povinnostech. In: *Facebook* [online]. Aktualizace 2011 [vid. 5. 3. 2012]. Dostupné z: http://www.facebook.com/legal/terms

[7] TWITTER. Prohlášení o právech a povinnostech. In: *Twitter* [online]. 2012 [vid. 5. 3. 2012]. Dostupné z: http://twitter.com/privacy

[8] KREJČÍ, V., KOPECKÝ, K. Nebezpečí elektronické komunikace 2. In: *Centrum prevence rizikové virtuální komunikace* [online]. 13. 2. 2011 [vid. 10. 1. 2012]. Dostupné z: http://www.prvok.upol.cz/index.php/ke-staeni/doc_download/13-nebezpei-elektronicke-komunikace-2-centrum-prvok-2011

[9] Co jsou sociální sítě? In: *Bezpečný internet.cz* [online]. Aktualizace 2012 [vid. 1. 2. 2012]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/socialni-site/co-jsou-socialni-site.aspx?kurz=true

[10] KOPECKÝ, K. Sociální sítě jako prostředí pro nebezpečnou virtuální komunikaci. In: *E-bezpečí* [online]. 17. 11. 2009 [vid. 20. 2. 2012]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/socialni-sit/147-222

[11] ČERMÁK, M. Proč mít rád Facebook. A proč se ho bát. In: *Lidovky.cz* [online]. 9. 2. 2009 [vid. 22. 2. 2012]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/socialni-sit/147-222

[12] WONG, P. Conversations About the Internet #5: Anonymous Facebook Employee. In: *The Rumpus* [online]. 11. 1. 2010 [vid. 20. 2. 2012]. Dostupné z: http://therumpus.net/2010/01/conversations-about-the-internet-5-anonymous-facebook-employee/?full=yes

[13] FACEBOOK. Fact Sheet. In: *Facebook* [online]. Aktualizace 2012 [vid. 13. 3. 2012]. Dostupné z: http://newsroom.fb.com/content/default.aspx?NewsAreaId=22

[14] SMITH, J. Facebook Surpasses 175 Million Users, Continuing to Grow by 600k Users/Day. In: *Inside Facebook* [online]. 14. 2. 2009 [vid. 13. 3. 2012]. Dostupné z: http://www.insidefacebook.com/2009/02/14/facebook-surpasses-175-million-users-continuing-to-grow-by-600k-usersday/

[15] LYONS, G. Facebook to Hit a Billion Users in the Summer. In: *icrossing* [online]. 11. 1. 2012 [vid. 13. 3. 2012]. Dostupné z: http://connect.icrossing.co.uk/facebook-hit-billion-users-summer_7709

[16] SYMANTEC. Fact Symantec Internet Security Threat Report Trends for 2010. In: *Symantec* [online]. Duben 2011 [vid. 14. 3. 2012]. Dostupné z: https://www4.symantec.com/mktginfo/downloads/21182883_GA_REPORT_ISTR_Main-Report_04-11_HI-RES.pdf

[17] DOČEKAL, D. Rizika sociálních sítí a Webu 3.0 v praxi. In: *Lupa.cz* [online]. 17. 2. 2010 [vid. 13. 3. 2012]. Dostupné z: http://www.lupa.cz/clanky/rizika-socialnich-siti-a-webu-3-0-v-praxi/

[18] BARKACS, L. L., aj. Do you think I'm sexty? Minors and sexting: teenage fad or child pornography? *Journal of Legal, Ethical and Regulatory Issues*. 2010, roč. 13, č. 2, s. 23–31.

[19] WILLARD, N. E. Sexting and Youth: Achieving Rational Response. *Journal of Social Sciences*. 2010, roč. 6, č. 4, s. 542-562.

[20] THE NATIONAL CAMPAIGN TO PREVENT TEEN AND UNPLANNED PREGNANCY. Sex and Tech. In: *The National Campaign to Prevent Teen and Unplanned Pregnanck* [online]. Aktualizováno 6. 1. 2009 [vid. 10. 3. 2012]. Dostupné z: http://www.thenationalcampaign.org/sextech/PDF/SexTech_Summary.pdf

[21] MITCHELL, K. J., aj. Prevalence and Characteristics of Youth Sexting: A National Study. *PEDIATRICS* [online]. 30. 12. 2011, roč. 129, č. 1, s. 13-20 [vid. 12. 3. 2012]. ISSN 0031-4005. Dostupné z: http://pediatrics.aappublications.org/cgi/doi/10.1542/peds.2011-1730

[22] HASALÍK, R. Hambaté Líbímseti.cz: fotografie nejsou osobní údaj. In: *Brouzdej.cz* [online]. 2005 [vid. 24. 2. 2012]. Dostupné z: http://brouzdej.cz/blogy/radimh/7062.html

[23] JAISHANKAR, K., aj. Cyber Stalking: A Global Menace in the Information Super Highway. *ERCES on-line Quarterly Review* [online]. 2005, roč. 2, č. 3 [vid. 7. 12. 2012]. ISSN 1811-9123. Dostupné z: http://www.erces.com/journal/articles/archives/volume2/v03/v02.htm

[24] KOPECKÝ, K. *Stalking a kyberstalking* [online]. Olomouc: NET UNIVERSITY, 2010. [vid. 10. 12. 2011]. ISBN 978-80-254-7737-3. Dostupné z: http://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/12-stalking-a-kyberstalking

[25] SPITZBERG, B. H., aj. Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society* [online]. 7. 1. 2011, roč. 4, č. 1, s. 67-88 [vid. 10. 3. 2012]. Dostupné z: http://www-rohan.sdsu.edu/~bsavatar/articles/Cyberstalking-NM&S02.pdf

[26] KOPECKÝ, K. *Kybergrooming* [online]. Olomouc: NET UNIVERSITY, 2010. [vid. 10. 12. 2011]. ISBN 978-80-254-7573-7. Dostupné z: http://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/11-kybergrooming

[27] TŘEČEK, Č, aj. Deviant Hovorka se dočkal za zneužití dvaceti chlapců mírnějšího trestu. In: *iDnes.cz* [online]. 26. 5. 2009 [vid. 20. 2. 2012]. Dostupné z: http://zpravy.idnes.cz/odvolaci-soud-rozhodne-o-trestu-za-zneuziti-jednadvaceti-chlapcu-p9q-/krimi.aspx?c=A090526_073207_krimi_cen

[28] CARTER, H. Merseyside police refers itself to IPCC over Facebook killer Peter Chapman. In: *theguardian* [online]. 9. 3. 2010 [vid. 20. 2. 2012]. Dostupné z: http://www.guardian.co.uk/uk/2010/mar/09/merseyside-police-peter-chapman-facebook

[29] SAFERINTERNET.CZ. Riziková komunikace online. In: *saferinternet.cz* [online]. Březen 2009 [vid. 23. 2. 2012]. Dostupné z: http://www.saferinternet.cz/webmagazine/download.asp?idg=58&file=2009_saferinternet_cz_66.pdf

[30] STOKES, P. Peter Chapman targeted thousands of young girls. In: *The Telegraph* [online]. 8. 3. 2010 [vid. 20. 2. 2012]. Dostupné z: http://www.telegraph.co.uk/news/uknews/crime/7397894/Peter-Chapman-targeted-thousands-of-young-girls.html

[31] KREJČÍ, V. *Kyberšikana* [online]. Olomouc: NET UNIVERSITY, 2010. [vid. 10. 12. 2011]. ISBN 978-80-254-7791-5. Dostupné z: http://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/13-kyberikana

[32] NYKODÝMOVÁ, H. Kde končí legrace a začíná kyberšikana. In: *Lupa.cz* [online]. 17. 8. 2007 [vid. 5. 3. 2012]. Dostupné z: http://www.lupa.cz/clanky/kde-konci-legrace-a-zacina-kybersikana/

[33] BAIO, A. Star Wars Kid: The Data Dump. In: *WAXY* [online]. Aktualizováno 14. 6. 2008 [vid. 1. 3. 2012]. Dostupné z: http://waxy.org/2008/05/star_wars_kid_the_data_dump/

[34] GRANGER, S. Social Engineering Fundamentals, Part I: Hacker Tactics. In: *Symantec* [online]. 18. 12. 2001 [vid. 13. 2. 2012]. Dostupné z: http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics

[35] ŠIMEK, R. *Sociotechnika (sociální inženýrství)* [online]. 2003 [vid. 22. 2. 2012]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm

[36] LASHKARI, A. H., aj. Shoulder Surfing attack in graphical password authentication. *International Journal of Computer Science and Information Security* [online]. 2009, roč. 6, č. 2, s. 145–154 [vid. 17. 2. 2012]. ISSN 1947-5500 Dostupné z: http://arxiv.org/ftp/arxiv/papers/0912/0912.0951.pdf

[37] *HOAX.cz* [online]. 2012 [vid. 13. 3. 2012]. Dostupné z: http://www.hoax.cz /

[38] SATRAPA, P. Phishing - nový trend v podvodných dopisech. In: *Lupa.cz* [online]. 20. 5. 2004 [vid. 18. 2. 2012]. Dostupné z: http://www.lupa.cz/clanky/phishing-novy-trend-v-podvodnych-dopisech/

[39] TRUSTEER. Measuring the Effectiveness of In-the-Wild Phishing Attacks. In: *TRUSTEER* [online]. 2. 12. 2009 [vid. 3. 3. 2012]. Dostupné z: http://www.trusteer.com/sites/default/files/Phishing-Statistics-Dec-2009-FIN.pdf

[40] FLORÊNCIO, D., aj. A LargeScale Study of Web Password Habits. In: *Microsoft Research* [online]. 22. 3. 2007 [vid. 8. 2. 2012]. Dostupné z: http://research.microsoft.com/pubs/74164/www2007.pdf

[41] MCCALL, T. Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks. In: *Gaertner* [online]. 17. 12. 2007 [vid. 24. 2. 2012]. Dostupné z: http://www.gartner.com/it/page.jsp?id=565125

[42] Phishing websites pocket $3 billion in China. In: *The Economic Times* [online]. 15. 1. 2011 [vid. 27. 2. 2012]. Dostupné z: http://articles.economictimes.indiatimes.com/2011-01-15/news/28425183_1_phishing-e-commerce-online-banking

[43] RASMUSSEN, R., aj. Global Phishing Survey: Trends and Domain Name Use in 1H2010. In: *APWG* [online]. Říjen 2010 [vid. 20. 2. 2012]. Dostupné z: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf

[44] KEIZER, G. Spear phishers sharpen skills, craft 'incredible' attacks, say experts. In: *Computerworld* [online]. 14. 6. 2011 [vid. 23. 2. 2012]. Dostupné z: http://www.computerworld.com/s/article/9217601/Spear_phishers_sharpen_skills_craft_incredible_attacks_say_experts

[45] DOČEKAL, D. Jak se dělá phishing. In: *Lupa.cz* [online]. 20. 3. 2008 [vid. 15. 2. 2012]. Dostupné z: http://www.lupa.cz/clanky/jak-se-dela-phishing/

[46] EMIGH, A. Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures. In: *APWG* [online]. 3. 10. 2005 [vid. 19. 2. 2012]. Dostupné z: http://www.antiphishing.org/Phishing-dhs-report.pdf

[47] APWG. Evolution of Phishing Attacks. In: *APWG* [online]. 7. 2. 2005 [vid. 3. 3. 2012]. Dostupné z: http://www.antiphishing.org/Evolution%20of%20Phishing%20Attacks.pdf

[48] SATRAPA, P. 10 zásad ochrany před phishingem. In: *Lupa.cz* [online]. 15. 4. 2010 [vid. 18. 2. 2012]. Dostupné z: http://www.lupa.cz/clanky/10-zasad-ochrany-pred-phishingem/

[49] TANASE, M. IP Spoofing: An Introduction. In: *Symantec* [online]. 11. 3. 2003 [vid. 10. 2. 2012]. Dostupné z: http://www.symantec.com/connect/articles/ip-spoofing-introduction

[50] HACHMAN, M. The Anonymous DDOS: A Tool of Last Resort?. In: *PCMAG.com* [online]. 27. 2. 2012 [vid. 5. 3. 2012]. Dostupné z: http://www.pcmag.com/article2/0,2817,2400842,00.asp

[51] BITTO, O. Rhybaření střídá pharming. In: *Lupa.cz* [online]. 31. 3. 2005 [vid. 17. 2. 2012]. Dostupné z: http://www.lupa.cz/clanky/rhybareni-strida-pharming/

[52] DOSTÁLEK, L., aj. *Velký průvodce protokoly TCP/IP: Bezpečnost*. 1.vyd. Praha: Computer Press, 2001. ISBN 80-722-6513-X.

[53] Spyware. In *Bezpečný internet.cz* [online]. 2011 [vid. 13. 2. 2012]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/zabezpeceni-pocitace/spyware.aspx

[54] SETTI, S. Introduction to Spyware Keyloggers. In: *Symantec* [online]. 2. 11. 2010 [vid. 15. 2. 2012]. Dostupné z: http://www.symantec.com/connect/articles/introduction-spyware-keyloggers

[55] THE IMPERVA APPLICATION DEFENSE CENTER. Consumer Password Worst Practices. In: *Imperva* [online]. 22. 3. 2007 [vid. 8. 2. 2012]. Dostupné z: http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf

[56] UPC ČESKÁ REPUBLIKA. UPC Fiber Power internet - přehled tarifů. In: *UPC Česká republika* [online]. 31. 3. 2012 [vid. 31. 3. 2012]. Dostupné z: http://www.upc.cz/internet/

[57] GRAMPP, F. T., aj. Unix Operating System Security. *AT&T Bell Laboratories Technical J. 1984,* roč. 63, č. 8, s. 1649–1672.

[58] Password Recovery Speeds. In: *LockDown* [online]. 10. 6. 2009 [vid. 23. 2. 2012]. Dostupné z: http://www.lockdown.co.uk/?pg=combi#Classes

[59] YAN, J., aj. Password Memorability and Security: Empirical Results. *IEEE Security and Privacy* [online]. 2004, roč. 2, č. 5, s. 25–31 [vid. 11. 2. 2012]. Dostupné z: http://homepages.cs.ncl.ac.uk/jeff.yan/jyan_ieee_pwd.pdf

[60] CONNECTSAFELY. Tips for Strong, Secure Passwords. In: ConnectSafely.org [online]. 2010 [vid. 20. 2. 2012]. Dostupné z: http://www.connectsafely.org/Safety-Tips/tips-to-create-and-manage-strong-passwords.html

[61] FFIEC. Authentication in an Internet Banking Environment. In: *FFIEC* [online]. 7. 10. 2005 [vid. 4. 3. 2012]. Dostupné z: http://www.ffiec.gov/pdf/authentication_guidance.pdf

[62] VÝZKUMNÝ ÚSTAV PEDAGOGICKÝ V PRAZE. *Rámcový vzdělávací program pro základní vzdělávání.* [online]. Praha: Výzkumný ústav pedagogický v Praze, 2007. [vid. 7. 2. 2012]. Dostupné z http://www.vuppraha.cz/wp-content/uploads/2009/12/RVPZV_2007-07.pdf

[63] VÝZKUMNÝ ÚSTAV PEDAGOGICKÝ V PRAZE. *Rámcový vzdělávací program pro základní vzdělávání: Pomůcka na pomoc učitelům.* [online]. Praha: Výzkumný ústav pedagogický v Praze, 2010. [vid. 7. 2. 2012]. Dostupné z http://www.vuppraha.cz/wp-content/uploads/2009/12/RVPZV-pomucka-ucitelum.pdf

[64] GYMNÁZIUM U BALVANU JABLONEC NAD NISOU. *Školní vzdělávací program pro základní vzdělávání, obor vzdělávání 79-41-K/81*. [online]. 1. 9. 2010 [vid. 12. 2. 2012]. Dostupné z http://gymjbc.cz/SVP/SVP_NG.pdf

[65] ZŠ ALOISINA VÝŠINA LIBEREC. *Školní vzdělávací program pro základní vzdělávání*. Liberec: ZŠ Aloisina Výšina, 2012.

[66] VANÍČEK, J., aj. *Informatika pro základní školy a víceletá gymnázia*. Vyd. 1. Brno: Computer Press, 2006. ISBN 80-251-1082-6.

[67] KOVÁŘOVÁ, L., aj. *Informatika pro základní školy*. Vyd. 2. Kralice na Hané: Computer Media, 2009. ISBN 978-80-7402-017-9.

[68] KALAŠ, I., aj. *Tvorivá informatika*. Vyd. 1. Bratislava: Slovenské pedagogické nakladateľstvo - Mladé letá, 2007. ISBN ISBN 978-80-10-00887-2.

[69] POSPÍŠIL, J., aj. *Mediální výchova*. Vyd. 1. Kralice na Hané: Computer Media, 2009. ISBN 978-807-4020-223.

[70] POSPÍŠIL, J. aj. *Mediální výchova*: *cvičebnice : řešení*. Vyd. 1. Kralice na Hané: Computer Media, 2010. ISBN 978-807-4020-551.

[71] POSPÍŠIL, J., aj.. *Mediální výchova*: *metodika*. Vyd. 1. Kralice na Hané: Computer Media, 2010. ISBN 978-807-4020-407.

[72] MIČIENKA, M., aj. *Základy mediální výchovy*. Vyd. 1. Praha: Portál, 2007. ISBN 978-807-3673-154.

[73] *E-bezpečí.cz* [online]. 2011 [vid. 14. 2. 2012]. Dostupné z: http://www.e-bezpeci.cz /

[74] *Sexting.cz* [online]. 2012 [vid. 25. 3. 2012]. Dostupné z: http://www.sexting.cz /

[75] *E-nebezpečí.cz* [online]. 2012 [vid. 14. 2. 2012]. Dostupné z: http://www.e-nebezpeci.cz /

[76] *Saferinternet.cz* [online]. 2011 [vid. 14. 2. 2012]. ISSN 1803-9219. Dostupné z: http://www.saferinternet.cz /

[77] *Bezpečně-online.cz* [online]. 2011 [vid. 15. 2. 2012]. Dostupné z: http://www.bezpecne-online.cz/

[78] *Bezpečnýinternet.cz* [online]. 2010 [vid. 15. 2. 2012]. Dostupné z:http://www.bezpecnyinternet.cz/

[79] Seznamsebezpečně.cz [online]. 2012 [vid. 22. 2. 2012]. Dostupné z: http://www.seznamsebezpecne.cz/

[80] ÚOOÚ. Soutěž "Moje soukromí! Nekoukat, nešťourat!". In: *ÚOOÚ* [online]. 28. 1. 2012 [vid. 17. 2. 2012]. Dostupné z: http://uoou.cz/uoou.aspx?menu=287&submenu=333

[81] *ConnectSafely.org* [online]. 2012 [vid. 15. 2. 2012]. Dostupné z: http://www.connecsafely.cz/

[82] *Safekids.com* [online]. 2012 [vid. 15. 2. 2012]. Dostupné z: http://www. safekids.com

[83] *Safeteens.com* [online]. 2012 [vid. 15. 2. 2012]. Dostupné z: http://www. safeteens.com

[84] *Saferinternet.org* [online]. 2012 [vid. 15. 2. 2012]. Dostupné z: http://www.saferinternet.org

[85] *Antiphishing.org* [online]. 2012 [vid. 15. 2. 2012]. Dostupné z: http://www.antiphishing.org

[86] APWG. Phishing Education Landing Page. In: *APWG* [online]. Srpen 2008 [vid. 7. 3. 2012]. Dostupné z: http://education.apwg.org/r/

[87] *Ovce.sk* [online]. 2012 [vid. 19. 2. 2012]. Dostupné z: http://www.ovce.sk

[88] *SecurityCartoon.com* [online]. 2007 [vid. 19. 2. 2012]. Dostupné z: http://www.*securitycartoon.com*

[89] *Privacyactivism.org* [online]. 2011 [vid. 19. 2. 2012]. Dostupné z: http://www.*privacyactivism.org*

[90] KALHOUS, Z., aj. *Školní didaktika*. Vyd. 1. Praha: Portál, 2002. ISBN 80-717-8253-X.

[91] ŘÍČAN, Pavel. *Psychologie*: *příručka pro studenty*. Vyd. 1. Praha: Portál, 2005. ISBN 80-717-8923-2.

[92] CHRÁSKA, Miroslav. *Metody pedagogického výzkumu*: *základy kvantitativního výzkumu*. Vyd. 1. Praha: Grada Publishing, 2007. ISBN 978-80-247-1369-4.

[93] CARTER, H. Facebook murderer who posed as teenager to lure victim jailed for life. In: *theguardian* [online]. 8. 3. 2010 [vid. 20. 2. 2012]. Dostupné z: http://www.guardian.co.uk/uk/2010/mar/09/merseyside-police-peter-chapman-facebook

Seznam tabulek

Seznam obrázků a grafů

Seznam příloh

Přílohy

Příloha A – Sexting v případech

Důsledky sextingu mohou být dvojího charakteru. Prvním jsou důsledky právního rázu, u nás je na šíření sexuálně explicitních materiálů, tedy fotografií, videí nebo deníků, které zahrnují osoby mladší 18 let, nahlíženo jako na tvorbu, šíření a přechovávání dětské pornografie. [74] V českých poměrech bylo šíření takových materiálů mladistvými potrestáno relativně mírně (případ z Měřína). [74] Praxe z USA se často liší, od alternativních trestů až po přísné potrestání Phillipa Alperta. [19 s. 546]

Druhý a dle mého vážnějším důsledek sextingu se týká toho, kdo byl na fotografii či videu vyobrazen (a kdo obvykle neuváženě takový materiál odeslal jako první), musí čelit společenské potupě a je obvykle terčem šikany a kyberšikany. Dva nejznámější případy s tragickým koncem pocházejí z USA, prvním z nich byl osud Jessie Logan, jejíž nahé fotografie dalším známým rozeslal její ex-přítel. [18 s. 23] Druhý případ se týká teprve 13 leté Hope Whitsell, která taktéž neuváženě poslala svou nahou fotografii chlapci, který se jí líbil, fotografii dále rozeslala chlapcova kamarádka a ta se začala šířit, Hope byla vystavena neustálému psychickému tlaku. [19 s. 557–558] Obě dívky psychický tlak nevydržely a spáchaly sebevraždu. V obou případech došlo taktéž k nešetrnému přístupu škol, jejichž žákyně se staly terčem šikany, v případě Hope reagovala škola kárným řízením, které tlak na oběť zvětšilo, v případě Jessie je škola napadána pro liknavý přístup k šikaně, které byla Jessie vystavena.

Příloha B – Analýza groomingového případu

Tento případ s tragickým koncem se odehrál v roce 2009 ve Velké Británii, obětí dříve odsouzeného devianta se stala 17 letá studentka Asleigh Hallová. Následující analýza je založena na informacích, které jsou uvedeny v článcích na serverech `Guardian.co.uk` a `Telegraph.co.uk`. [28] [30] [93]

Hlavní důvody, proč byl útok úspěšný, se dají shrnout do několika bodů a často potvrzují výše zmiňované metody a triky groomerů.

1) Chapman si vytvořil věrohodný profil na Facebooku, Netlogu a dalších sociálních sítích, kde se prezentoval jako atraktivní 17 letý mladík, měl však i další identity.
2) Udržoval si síť přátel, kde bylo 3000 dívek a žen ve věku 13 až 31 let.
3) K získávání údajů o nich použil i dotazníku, kde byly otázky mířené i na velmi intimní údaje, na který mu děvčata často odpověděla (mini aplikace a otázky na Facebooku mají také takový potenciál).
4) Dovolil si zasílat i sexuálně laděné příspěvky, které měly pozitivní ohlas.
5) Asleigh měla údajně nízké sebevědomí, což je fakt, který predátorům často nahrává.
6) Ke komunikaci s ní používal nejen Facebook, ale i MSN či sociální síť `Tagged.com`
7) Oznámil jí, že při osobní schůzce ji autem vyzvedne otec jeho falešné identity (ve skutečnosti tedy on osobně).

Příloha C – Zachycený nekvalitní phishingový e-mail

Received: from ma.nwps.kh.edu.tw (ma.nwps.kh.edu.tw [163.32.209.5]) by email-smtpd7.ng.seznam.cz (Seznam SMTPD 1.2.15-6@18976) with ESMTP; Wed, 01 Feb 2012 05:33:24 +0100 (CET)
Received: from ma.nwps.kh.edu.tw ([127.0.0.1]) by ma.nwps.kh.edu.tw (8.14.1/8.14.1) with ESMTP id q114QQZj003935; Wed, 1 Feb 2012 12:26:26 +0800
From: =?us-ascii?Q?Chevron=20Oil=20=26=20Gas=20Company?= <info@oil.com>
Reply-To: remetancefirmc2011@hotmail.com
Subject: =?iso-8859-2?Q?Va=9Ae=20overovac=ED=20c=EDslo=20je=3A=20=28CB2009=2D100=2F69=29?=
Date: Wed, 01 Feb 2012 05:26:26 +0100 (CET)
Message-Id: <20120201042638.M14697@oil.com>
X-Mailer: OpenWebMail 2.52 20060502
X-Originatingip: 180.74.127.89 (nw80)
Mime-Version: 1.0
Content-Type: text/plain; charset=iso-8859-1
X-Greylist: Sender IP whitelisted, not delayed by milter-greylist-2.1.12 (ma.nwps.kh.edu.tw [127.0.0.1]); Wed, 01 Feb 2012 12:26:38 +0800 (CST)
X-Smtpd: 1.2.15-6@18976
X-Session: 786
X-Country: TW
X-Virus-Info:clean
X-Seznam-Spf:neutral
X-Seznam-Domainkeys:neutral
X-Spam-Bar:+++
X-Spam-Status:score=3.6
X-Seznam-Ffp: -1432111751

CHEVRON ropy / plynu AWARD oznámení:

To je informovat Vás, □e Chevron udelila vám soucet £ 170,152.000.00
 Liber za rok 2011 tento prínos, pro vás a va□i rodinu na□ich □ivotu
 k minulosti. Tento e-mail je nastaven na 3 □tastní výherci vybráni náhodne na
 120.000.00 e-mailových úctu na celém svete. Va□e overovací císlo je: (CB2009-100/69)
 Pochopte prosím, □e tato podpora není ani v lote-rii, ani hraní vítezství
 je to jen výhoda, která byla organizována CHEVRON olej / plyn-spolecnost.
 Chcete-li podat své □ádosti, obratte

se na likvidaci pojistných událostí dustojník
 e-mail / telefonický kontakt uveden ní□e:

Likvidaci pojistných událostí mluvcí:
Pan Jeffery Wilford
Tel: +234-818-521-3052
EMAIL: remetancefirmc2011@hotmail.com

Doporucujeme, aby mu:

Jména a príjmení:
KONTAKTNÍ ADRESA:
VEK:
Národnost:
PHONE:
FAX:
mobil:
SEX (M / F):
POZNÁMKY CHEVRON:

Jsme rádi, □e jste jako jeden z na□ich luckly vítezu.

S pozdravem
MR. Osivo flow
Zonální koordinátor

Příloha D – Plán ukázkové hodiny

Cíl hodiny: Na konci hodiny žáci ocení zásady ochrany osobních údajů jako užitečné a jejich aplikaci v praxi budou považovat za přínosnou (cíl zastřešující a počítající s dílčími cíli a jejich naplnění viz podrobný plán).

Téma a obsah: Zásady ochrany osobních údajů na internetu, metody útoku a jak se jim bránit.

Čas: Lekce je plánována na 45 minut, jednotlivé aktivity jsou sice podrobně časově rozplánovány, jsou však pouze orientační, lektor musí být dostatečně flexibilní a plán dle potřeb žáků upravovat přímo v hodině. Problematika by si zasloužila větší časovou dotaci a aktivity je možné rozšiřovat a doplňovat.

Fáze: Lekce obsahuje motivační a expoziční fázi, fixace probíhá pouze u samostatné práce s hesly, jako fixaci můžeme do jisté míry chápat každodenní používání internetu, kdy v různé míře dochází k rozhodování o aplikaci poznatků z této hodiny. Drobná fixační cvičení by bylo vhodné zahrnout i v rámci další vyučovací hodiny.

Metody: Viz plán.

Organizační formy: Viz plán.

Vstupní znalosti žáků: Základy práce s počítačem, internetovým prohlížečem a elektronickou poštou. Pochopení základů autentizace (přihlašování přes jméno a heslo). Znalost prostředí sociálních sítí (není nutná, ale může pomoci stimulovat žáky k diskusi, otázkám…)

Reflexe: Analýza zpětné vazby a reflexe je provedena v rámci praktické části práce.

Čas (min)	**Cíle, metoda, forma, fáze, obsah a popis aktivity**	**Poznámky, pomůcky**
0–1	**Obsah:** Seznámení s cílem hodiny. **Metoda:** Slovní – monologická. **Organizační forma:** Frontální výuka. **Fáze:** Motivace.	

2–3	**Obsah:** Představení se lektora (pod falešným jménem) a vyzvídání osobních údajů na žácích, upozornění na odlišnost vnímání v „reálném“ a online světě a připraví pomyslný můstek pro vkročení do problematiky ochrany osobních údajů na internetu. **Metoda:** Slovní – dialogická (rozhovor, představení se). **Fáze:** Motivace. **Cíl:** Žák si uvědomí možný rozpor mezi chováním online a v „reálném světě“ (afektivní).	
4–6	**Obsah:** Co na sebe sdílím, co na sebe sdílejí ostatní, jsou údaje vždy pravdivé? Demonstrace na příkladech z praxe (reálné profily na soc. sítích, tvorba falešné identity) a odtajnění skutečné identity lektora (opět s návazností na alteraci identity v „reálném světě“ a na internetu, složitost tohoto procesu). **Metoda:** Slovní – monologická (výklad). **Organizační forma:** Frontální výuka. **Fáze:** Expozice. **Cíl:** Žák vnímá možný rozpor mezi skutečnou a fiktivní identitou a čím je tento rozpor způsoben. (afektivní) Žák dokáže vysvětlit, proč je na internetu snazší tvořit a prezentovat falešnou identitu. (kognitivní)	
7–10	**Obsah:** Seznámení s příběhem Ashleigh Hallové, ukázka technik kybergroomingu a role osobních údajů (mirroring). **Metoda:** Slovní – monologická (příběh), dialogická (ukázka mirroringu). **Organizační forma:** Frontální výuka. **Fáze:** Expozice. **Cíl:** Žák akceptuje skutečnost, že jeho osobní údaje a informace mohou být využity proti němu. (afektivní) Žák dokáže objasnit, jak postupoval útočník v prezentovaném příběhu a proč byl úspěšný. (kognitivní)	
11–15	**Obsah:** Interaktivní rekonstrukce sextingového případu Hope Witsell. Existují nějaké bezpečné údaje? Proč bych měl přemýšlet, než něco odešlu či zveřejním. **Metoda:** Slovní – monologická s prvky interaktivity (příběh). **Organizační forma:** Frontální výuka. **Fáze:** Expozice. **Cíl:** Žák je přesvědčen o skutečnosti, že zveřejnění osobního údaje nebo materiálu s osobní tematikou (fotografie) se může obrátit proti němu nebo ho dostat do nepříjemné situace. (afektivní)	

16–19	**Obsah:** Problematika bezpečnosti hesel, metody jejich získání a prolamování, zásady tvorby kvalitního hesla, nástroje pro pomoc s hesly (manažery, ověření síly hesla – `Passwordmeter.com`). **Metoda:** Slovní – monologická (výklad). **Organizační forma:** Frontální výuka. **Fáze:** Expozice. **Cíl:** Žák dokáže vyjmenovat a vlastními slovy vysvětlit, jak může útočník získat heslo. (kognitivní)	
20–23	**Obsah:** Zásady tvorby kvalitního hesla (heslo vyprávějící příběh), nástroje pro pomoc s hesly (manažery, online nástroj pro ověření síly hesla `Passwordmeter.com`). **Metoda:** Slovní – monologická (výklad). Instruktáž. **Organizační forma:** Frontální výuka. **Fáze:** Expozice. **Cíl:** Žák dokáže vytvořit vlastní bezpečné a zapamatovatelné heslo za pomoci metody – heslo vypráví příběh. (kognitivní)	Online nástroj pro ověření síly hesla.
24–29	**Obsah:** Žáci si samostatně vyzkoušejí online nástroj pro ověřování síly hesel. Mohou si ověřit i vlastní heslo, či jiné často používané výrazy. **Metoda:** (Žáci individuálně pracují) **Organizační forma:** Individuální práce. **Fáze:** Fixace. **Cíl:** Žák dokáže s pomocí online nástroje pro ověřování síly hesel analyzovat heslo a rozhodnout o jeho bezpečnosti. (kognitivní) Žák je přesvědčen o užitečnosti používání kvalitního hesla. (afektivní, postupně budováno během předchozích aktivit)	Online nástroj pro ověření síly hesla.
30–36	**Obsah:** Úvod do problematiky phishingových zpráv. Druhy phishingových zpráv a metody, které používají. **Metoda:** Inscenační (žák vyhrává milion korun českých), Dialogické - heuristický rozhovor. **Organizační forma:** Frontální výuka. **Fáze:** Expozice. **Cíl:** Žák dokáže uvést příklady metod, které využívají podvodné phishingové zprávy. (kognitivní) Žák dokáže kriticky zkoumat zprávu na základě známých phishingových metod a určit zda by se mohlo jednat o zprávu podvodnou. (kognitivní)	Ukázka podvodné zprávy.
37–43	**Obsah:** Co je to HTTPS? Jeho využití při internetové komunikaci. **Metoda:** Slovní – monologická (výklad). **Organizační forma:** Frontální výuka. **Fáze:** Expozice. **Cíl:** Žák dokáže vlastními slovy popsat, co to znamená, že komunikace je zabezpečená pomocí protokolu HTTPS. (kognitivní) Žák dokáže vědomě využít protokolu HTTPS pokud je nabízen a uvědomuje si jeho výhody. (kognitivně-afektivní)	Navazuje na phishingovou zprávu.
44–45	**Poděkování za pozornost, vybídnutí k opatrnosti a využívání rozumu při internetové komunikaci, časová rezerva.**	

Příloha E – Znění dotazníku a metodika hodnocení odpovědí

Kurzivou jsou v této příloze psané komentáře, ty se týkají zejména bodového hodnocení jednotlivých odpovědí.

*** Povinné pole**

! Bodované pole

1. Jsi chlapec nebo dívka? *

- ○ Chlapec.
- ○ Dívka.

2. Kolik je ti let? *

Výběr: 11–17

3. Do jakého ročníku chodíš? *

- ○ 6. ročník.
- ○ 9. ročník.

4. Jsi žákem základní školy nebo nižšího gymnázia? *

- ○ Základní školy.
- ○ Nižšího gymnázia.

5. Kolik ročníků informačních a komunikačních technologií (nebo jiného na práci s počítači zaměřeného předmětu) jsi ve škole absolvoval? *

- ○ 0
- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5 a více

6. Jaká byla tvoje nejlepší známka na vysvědčení z informačních a komunikačních technologií (nebo obdobného předmětu)? *

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ Nikdy jsem neměl předmět informační a komunikační technologie.

7. Jaká byla tvoje nejhorší známka na vysvědčení z informačních a komunikačních technologií (nebo obdobného předmětu)? *

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ Nikdy jsem neměl předmět informační a komunikační technologie.

8. Na jakých sociálních sítích máš účet? Pokud máš účet i na jiných sociálních sítích, než jsou zde uvedené, vypiš je. *

- ☐ Facebook.com
- ☐ Líbímseti.cz
- ☐ xTeen.cz
- ☐ Lidé.cz
- ☐ Spolužáci.cz
- ☐ Twitter.com
- ☐ Bebo.com
- ☐ Badoo.com
- ☐ MySpace.com
- ☐ Nemám účet na žádné sociální síti
- ☐ Jiné: [ ]

9. Četl jsi podmínky užívání sociální sítě, na které máš účet? *

- ○ Ano.
- ○ Začal(a) jsem, ale nedočetla jsem je.
- ○ Ne.
- ○ Nemám účet na žádné sociální síti.

Následující 3 otázky vyplň pouze pokud máš účet na sociální síti Facebook.com.

10. Víš o možnosti nastavit si, co z tvých dat na Facebooku vidí (tzv. nastavení soukromí). Odpovídej, pouze pokud máš účet na Facebooku.

- ○ Ano.
- ○ Ne.

11. Využíváš této možnosti? Odpovídej, pouze pokud máš účet na Facebooku.

- ○ Ano.
- ○ Ne.

12. Která tvrzení o tvých přátelích na Facebooku platí? Zatrhni všechny pravdivé odpovědi. Odpovídej, pouze pokud máš účet na Facebooku.

Pokud jsou mezi tvými přáteli blízcí kamarádi, spolužáci a jiní vrstevníci, které znáš od pohledu ze školy, zatrhni první 3 odpovědi.

- ☐ Přátelím se s opravdu blízkými lidmi (kamarádi, kamarádky a rodina).
- ☐ Přátelím se s lidmi, které osobně znám (např. spolužáci, spoluhráči z týmu).
- ☐ Přátelím se s lidmi, které vídám, ale neznáme se osobně (např. viděl jsem ho s kamarádem, chodí k nám do školy, je to kluk spolužačky).
- ☐ Přátelím se s přáteli přátel, i když je jinak neznám.
- ☐ Přátelím se s kýmkoliv, kdo má podobný zájem vyplněný v profilu (např. hrajeme stejný sport, posloucháme stejného hudebního interpreta).
- ☐ Přátelím se s kýmkoliv, kdo mi pošle nabídku k přátelství a je to můj vrstevník.
- ☐ Přátelím se s kýmkoliv, kdo mi pošle nabídku k přátelství a nevypadá podezřele.
- ☐ Přátelím se s kýmkoliv, kdo mi pošle nabídku k přátelství.

13. Jaké údaje o sobě zveřejňuješ na internetu (do profilů na sociálních sítí, na svůj blog, na seznamku atp.)? Zatrhni všechna pravdivá tvrzení. *!

- ☐ Jméno.
- ☐ Příjmení.
- ☐ Měsíc a den narození (kdy máš narozeniny).
- ☐ Věk (případně rok narození).
- ☐ Město, kde bydlíš.
- ☐ Škola, na kterou chodíš.
- ☐ Fotografii svého obličeje.
- ☐ Karikaturu svého obličeje.
- ☐ Adresu, kde bydlíš.
- ☐ Své telefonní číslo.
- ☐ E-mailovou adresu.
- ☐ Kontaktní údaj na ICQ, Skype, MSN, AIM atp.
- ☐ Rodné číslo
- ☐ Žádný z uvedených údajů

*Tato otázka byla bodována trestnými body, byl zohledňován počet zveřejňovaných údajů a to takto: 0–4 údaje **0 b.**, 5–9 údajů **1 b.**, 10 a více údajů **2 b.** Údaje, které mohou vést k přímenému vystopování (kompletní adresa, jméno a příjmení) byly penalizovány **1 b.** Zveřejňování tel. čísla také **1 b.** Zveřejňování rodného čísla bylo penalizováno dalšími **2 b.** Celkem bylo možné získat až **6** trestných bodů.*

14. Zveřejňování kterých údajů považuješ za nebezpečné? Zatrhni všechny údaje, jejichž zveřejnění považuješ za nebezpečné. *

- ☐ Jméno.
- ☐ Příjmení.
- ☐ Měsíc a den narození (kdy máš narozeniny).
- ☐ Věk (případně rok narození).
- ☐ Město, kde bydlíš.
- ☐ Škola, na kterou chodíš.
- ☐ Fotografii svého obličeje.
- ☐ Karikaturu svého obličeje.
- ☐ Adresu, kde bydlíš.
- ☐ Své telefonní číslo.
- ☐ E-mailovou adresu.
- ☐ Kontaktní údaj na ICQ, Skype, MSN, AIM atp.
- ☐ Rodné číslo.
- ☐ Zveřejnění žádného z výše uvedených údajů není nebezpečné (Jinými slovy, poskytování těchto údajů je bezpečné).

15. Přihlásil se už někdo jiný s tvým vědomím a souhlasem na tvůj elektornický účet (e-mail, profil na sociální síti atp.)? Tzn. půjčil si mu svůj účet? *!

- ○ Ano.
- ○ Ne.

*Tato otázka byla bodována trestnými body, pokud respondent půjčil svůj účet někomu jinému, byl penalizován **1 b.***

16. Prolomil a zneužil už někdy někdo tvůj elektronický účet (e-mail, profil na sociální síti atp.)? Tzn. zjistil tvé přihlašovací údaje a ukradl ti účet nebo toho jinak zneužil? *!

- ○ Ano.
- ○ Ne.

*Tato otázka byla bodována trestnými body, pokud byl již někdy respondentům účet prolomen, byl penalizován **1 b.***

17. Myslíš si, že heslo nebo hesla, která používáš, jsou bezpečná? *

- ○ Ano.
- ○ Ne.

18. Používáš pro každý elektronický účet jiné heslo? *!

- ○ Ano.
- ○ Ne, mám stejné heslo na všechny účty.
- ○ Ne, ale mám více než jedno.

*Tato otázka byla bodována trestnými body, pokud respondent používá pro každý účet unikátní heslo, získal **0** **b.**, pokud používá více hesel, ale na některé účty používá hesla totožná, byl penalizován **1 b.**, pokud má na všech účtech stejné heslo, byl penalizován **2 b.***

19. Používáš nějaký nástroj na ověření síly hesla (např. Passwordmeter)? *

- ○ Ano.
- ○ Ne.

20. Znáš nějaké programy pro správu hesel? *

- ○ Ano.
- ○ Ne.

21. Používáš správce hesel? *

- ○ Ano.
- ○ Ne.

22. Která tvrzení platí o tvém nejčastěji používaném hesle (zadáváš ho nejčastěji nebo ho máš na nejvíce účtech)? Zatrhni všechna pravdivá tvrzení. *!

Pokud je tvé heslo např. „Pravda2“, zatrhni, že obsahuje velká písmena (P), malá písmena (ravda), čísla (2) a také, že slovo Pravda má význam.

- ☐ Obsahuje malá písmena.
- ☐ Obsahuje velká písmena.
- ☐ Obsahuje čísla.
- ☐ Obsahuje speciální znaky (např. % & ? !).
- ☐ Obsahuje nějaké slovo, které má význam (např. motorka, chameleon, Andrea, heslo7).
- ☐ Je kratší nebo rovno 6 znakům. (např. poleno, hrnec7, abc27).

*Tato otázka byla bodována trestnými body, pokud je respondentovo heslo kratší nebo rovno 6 znakům je penalizován **1 b.**, pokud obsahuje slovo, které má význam, je penalizován **1 b.** Podle počtu použití malých a velkých písmen, čísel a speciálních znaků v hesle byly přidělovány trestné body takto: Pouze 1 kategorie – **2 b.**, 2 kategorie – **1 b.**, 3 a 4 kategorie – **0 b.** Celkové maximum činilo **4 b,** čím méně bodů tím bezpečnější heslo.*

*Př.: JIk72!aj (**0 b.**), Motorka5 (**1 b.**), tranSporter (**2 b.**), Trubka (**3 b.**), heslo (**4 b.**).*

23. Komu sděluješ a kam si ukládáš své nejpoužívanější heslo? Zatrhni všechna pravdivá tvrzení. *!

- ☐ Znají ho moji rodiče nebo jeden z rodičů.
- ☐ Zná ho můj nejlepší kamarád/kamarádka.
- ☐ Zná ho někdo jiný (kamarádi/kamarádky, vedoucí na kroužku, někdo s kým chatuju atp.)
- ☐ Znám ho jen já.
- ☐ Mám ho napsané a vystavené u počítače.
- ☐ Mám ho zapsané v nešifrovaném dokumentu v počítači (např. v textovém souboru).
- ☐ Mám ho uložené na jiném médiu (např. na flash disku).
- ☐ Mám ho uložené ve správci hesel.
- ☐ Mám ho napsané a schované (např. na lístečku, v sešitě, v knize).
- ☐ Nikde ho nemám zapsané, pamatuji si ho.

*Tato otázka byla bodována trestnými body, každý z následujících nebezpečných návyků spojených s uchováváním a sdělováním hesla byl penalizován **1 b.** Maximum bylo **4 b.***

1) *Mám ho napsané a vystavené u počítače. **(1 b.)***
2) *Mám ho zapsané v nešifrovaném dokumentu v počítači (např. v textovém souboru). **(1 b.)***
3) *Zná ho můj nejlepší kamarád/kamarádka. **(1 b.)***
4) *Zná ho někdo jiný (kamarádi/kamarádky, vedoucí na kroužku, někdo s kým chatuju atp.) **(1 b.)***

24. Kdybys měl(a) zvolit z následujících hesel to nejbezpečnější, které by to bylo? *!

- ○ motorka
- ○ Vlak12
- ○ Panacek5
- ○ M!!p2o9
- ○ hlgfn
- ○ 12345678

*Tato otázka byla bodována trestnými body, dle metodiky u otázky 22, výjimkou bylo dodatečné penalizování hesla „12345678“ celkem na **4 b.**, protože se jedná velmi často používanou kombinaci složenou z po sobě jdoucích znaků (pouze čísel).*

*Bodování bylo pro úplnost takovéto: motorka (**3 b.**), Vlak12 (**2 b.**), Panacek5 (**1 b.**), M!!p2o9 (**0 b.**), hlgfn (**3 b.**), 12345678 (**4 b.**).*

25. Když stránka začíná https místo http (např. https://www.facebook.com/), znamená to, že: *!

- ○ se jedná o podvodnou stránku, kterou se někdo pravděpodobně snaží získat moje přihlašovací údaje.
- ○ se jedná o stránku, která může obsahovat obsah nevhodný pro děti a mládež.
- ○ se na můj účet snažil přihlásit někdo cizí.
- ○ je stránka možná infikovaná a bude potřeba ji před použitím zkontrolovat antivirovým programem.
- ○ je přenos dat zabezpečený šifrováním (kdyby někdo „poslouchal“, nebude tomu rozumět).

*Tato otázka byla bodována trestnými body, všechny odpovědi kromě té správné (je přenos dat zabezpečený šifrováním (kdyby někdo „poslouchal“, nebude tomu rozumět).) byly penalizovány **1 b.***

Právě ti přišel do e-mailové schránky tento dopis:

Odesilatel: soutez@apple.com

Zdarec,

pořádáme soutěž pro všechny teenagery a teenagerky o 10 iPhonů. Vybrali jsme tvoji mailovou adresu z tisíců jiných a teď jsi v užším finále!

Pro 5 nejrychlejších z Vás, kteří správně odpoví, je připraven nejnovější iPhone (aby bylo všechno fér, posílali jsme všechny maily současně)!

O zbylých 5 iPhonů se bude losovat ze všech správných odpovědí. Šance na výhru je opravdu vysoká!

Soutěžní otázka: Jak se jmenuje nejnovější iPhone od firmy Apple?

a) iPhone 650
b) iPhone XL
c) iPhone 4S

Stačí poslat správnou odpověď a kontaktní údaje a výhra může být jen tvoje!

Správná odpověď:

Jméno a příjmení:

Adresa bydliště:

Rodné číslo:

Telefonní číslo:

V případě dotazů volej naši hotlinku+420 741 548 653, ale bacha, soutěž trvá jen dva dny, kdo zaváhá, nevyhrává!

Za firmu Apple Inc.

Petr Urban

26. Jak bys zareagoval(a)? *!

- ○ Raději bych si zavolal(a) na kontaktní telefon, jestli to není omyl nebo podvod.
- ○ Hned bych vyplnil(a) potřebné údaje a odpověděl(a).
- ○ Neodpovídal(a) bych, je to podvod.

*Tato otázka byla bodována trestnými body, okamžitá odpověď a vyplnění údajů bylo penalizovány **2 b**., volání na linku uvedenou v podvodném mailu (podvodná v lepším případě neexistující linka) bylo penalizováno **1 b.***

Příloha F – Dotazníkové šetření v tabulkách

Pohlaví	Četnost (n_i)	Relativní četnost (f_i)
Chlapci	141	49 %
Děvčata	147	51 %

Tabulka F.1: Pohlaví respondentů – otázka č. 1 (celý vzorek, n = 288).

Pohlaví	Četnost (n_i)	Relativní četnost (f_i)
Chlapci	59	47 %
Děvčata	67	53 %

Tabulka F.2: Pohlaví respondentů – otázka č. 1 (pouze 6. ročníky, n = 126).

Pohlaví	Četnost (n_i)	Relativní četnost (f_i)
Chlapci	82	51 %
Děvčata	80	49 %

Tabulka F.3: Pohlaví respondentů – otázka č. 1 (pouze 9. ročníky, n = 162).

Pohlaví	Četnost (n_i)	Relativní četnost (f_i)
Chlapci	39	44 %
Děvčata	49	56 %

Tabulka F.4: Pohlaví respondentů – otázka č. 1 (kontrolní skupina po výuce, n = 88).

Věk	Četnost (n_i)	Relativní četnost (f_i)
11	40	14 %
12	81	28 %
13	9	3 %
14	63	22 %
15	88	31 %
16	6	2 %
17	1	0 %

Tabulka F.5: Věk respondentů – otázka č. 2 (celý vzorek, n = 288).

Věk	Četnost (n_i)	Relativní četnost (f_i)
11	40	32 %
12	81	64 %
13	4	3 %
14	1	1 %

Tabulka F.6: Věk respondentů – otázka č. 2 (pouze 6. ročníky, n = 126).

Věk	Četnost (n_i)	Relativní četnost (f_i)
13	5	3 %
14	62	38 %
15	88	54 %
16	6	4 %
17	1	1 %

Tabulka F.7: Věk respondentů – otázka č. 2 (pouze 9. ročníky, n = 162).

Věk	Četnost (n_i)	Relativní četnost (f_i)
11	12	14 %
12	41	47 %
13	5	6 %
14	12	14 %
15	17	19 %
16	1	1 %

Tabulka F.8: Věk respondentů – otázka č. 2 (kontrolní skupina po výuce, n = 88).

Ročník	Četnost (n_i)	Relativní četnost (f_i)
6. ročník	126	44 %
9. ročník	162	56 %

Tabulka F.9: Ročník, který respondenti navšěivují – otázka č. 3 (celý vzorek, n = 288).

Ročník	Četnost (n_i)	Relativní četnost (f_i)
6. ročník	58	66 %
9. ročník	30	34 %

Tabulka F.10: Ročník, který respondenti navštěvují – otázka č. 3 (kontrolní skupina po výuce, n = 88).

Typ školy	Četnost (n_i)	Relativní četnost (f_i)
Základní škola	192	67 %
Nižší gymnázium	96	33 %

Tabulka F.11: Typ školy, který respondenti navštěvují – otázka č. 4 (celý vzorek, n = 288).

Typ školy	Četnost (n_i)	Relativní četnost (f_i)
Základní škola	90	71 %
Nižší gymnázium	36	29 %

Tabulka F.12: Typ školy, který respondenti navštěvují – otázka č. 4 (pouze 6. ročníky, n = 126).

Typ školy	Četnost (n_i)	Relativní četnost (f_i)
Základní škola	102	63 %
Nižší gymnázium	60	37 %

Tabulka F.13: Typ školy, který respondenti navštěvují – otázka č. 4 (pouze 9. ročníky, n = 162).

Typ školy	Četnost (n_i)	Relativní četnost (f_i)
Základní škola	43	49 %
Nižší gymnázium	45	51 %

Tabulka F.14: Typ školy, který respondenti navštěvují – otázka č. 4 (kontrolní skupina po výuce, n = 88).

Počet ročníků ICT	Četnost (n_i)	Relativní četnost (f_i)
0	31	11 %
1	68	24 %
2	99	34 %
3	63	22 %
4	15	5 %
5 a více	12	4 %

Tabulka F.15: Počet ročníků ICT, který respondenti absolvovali – otázka č. 5 (celý vzorek, n = 288).

Počet ročníků ICT	Četnost (n_i)	Relativní četnost (f_i)
0	30	24 %
1	49	39 %
2	30	24 %
3	12	10 %
4	1	1 %
5 a více	4	3 %

Tabulka F.16: Počet ročníků ICT, který respondenti absolvovali – otázka č. 5 (pouze 6. ročníky, n = 126).

Počet ročníků ICT	Četnost (n_i)	Relativní četnost (f_i)
0	1	1 %
1	19	12 %
2	69	43 %
3	51	31 %
4	14	9 %
5 a více	8	5 %

Tabulka F.17: Počet ročníků ICT, který respondenti absolvovali – otázka č. 5 (pouze 9. ročníky, n = 162).

Počet ročníků ICT	Četnost (n_i)	Relativní četnost (f_i)
0	19	22 %
1	20	23 %
2	42	48 %
3	6	7 %
4	1	1 %

Tabulka F.18: Počet ročníků ICT, který respondenti absolvovali – otázka č. 5 (kontrolní skupina po výuce, n = 88).

Nejlepší známka z ICT	Četnost (n_i)	Relativní četnost (f_i)
1	224	78 %
2	22	8 %
3	9	3 %
4	2	1 %
5	0	0 %
Neměl(a) dosud ICT či obdobný předmět	31	11 %
Počet žáků, kteří již měli ICT či obdobný předmět	257	89 %
Aritmetický průměr ($\bar{x}$)	1,18	
Směrodatná odchylka (σ)	0,51	
Medián ($\tilde{x}$)	1	
Variační koeficient (V)	43 %	

Tabulka F.19: Nejlepší známka z ICT na vysvědčení, kterou respondenti dostali – otázka č. 6 (celý vzorek, n = 288).

Nejlepší známka z ICT	Četnost (n_i)	Relativní četnost (f_i)
1	86	68 %
2	6	5 %
3	3	2 %
4	1	1 %
5	0	0 %
Neměl(a) dosud ICT či obdobný předmět	30	24 %
Počet žáků, kteří již měli ICT či obdobný předmět	96	76 %
Aritmetický průměr ($\bar{x}$)	1,16	
Směrodatná odchylka (σ)	0,51	
Medián ($\tilde{x}$)	1	
Variační koeficient (V)	44 %	

Tabulka F.20: Nejlepší známka z ICT na vysvědčení, kterou respondenti dostali – otázka č. 6 (pouze 6. ročníky, n = 126).

Nejlepší známka z ICT	Četnost (n_i)	Relativní četnost (f_i)
1	138	85 %
2	16	10 %
3	6	4 %
4	1	1 %
5	0	0 %
Neměl(a) dosud ICT či obdobný předmět	1	1 %
Počet žáků, kteří již měli ICT či obdobný předmět	161	99 %
Aritmetický průměr ($\bar{x}$)	1,19	
Směrodatná odchylka (σ)	0,52	
Medián ($\tilde{x}$)	1	
Variační koeficient (V)	44 %	

Tabulka F.21: Nejlepší známka z ICT na vysvědčení, kterou respondenti dostali – otázka č. 6 (pouze 9. ročníky, n = 162).

Nejlepší známka z ICT	Četnost (n_i)	Relativní četnost (f_i)
1	63	72 %
2	4	5 %
3	2	2 %
4	0	0 %
5	0	0 %
Neměl(a) dosud ICT či obdobný předmět	19	22%
Počet žáků, kteří již měli ICT či obdobný předmět	69	78%
Aritmetický průměr ($\bar{x}$)	1,12	
Směrodatná odchylka (σ)	0,40	
Medián ($\tilde{x}$)	1	
Variační koeficient (V)	36 %	

Tabulka F.22: Nejlepší známka z ICT na vysvědčení, kterou respondenti dostali – otázka č. 6 (kontrolní skupina po výuce, n = 88).

Nejhorší známka z ICT	Četnost (n_i)	Relativní četnost (f_i)
1	171	59 %
2	46	16 %
3	30	10 %
4	8	3 %
5	2	1 %
Neměl(a) dosud ICT či obdobný předmět	31	11 %
Počet žáků, kteří již měli ICT či obdobný předmět	257	89 %
Aritmetický průměr ($\bar{x}$)	1,54	
Směrodatná odchylka (σ)	0,87	
Medián ($\tilde{x}$)	1	
Variační koeficient (V)	56 %	

Tabulka F.23: Nejhorší známka z ICT na vysvědčení, kterou respondenti dostali – otázka č. 7 (celý vzorek, n = 288).

Nejhorší známka z ICT	Četnost (n_i)	Relativní četnost (f_i)
1	71	56 %
2	17	13 %
3	5	4 %
4	2	2 %
5	1	1 %
Neměl(a) dosud ICT či obdobný předmět	30	24 %
Počet žáků, kteří již měli ICT či obdobný předmět	96	76 %
Aritmetický průměr ($\bar{x}$)	1,38	
Směrodatná odchylka (σ)	0,77	
Medián ($\tilde{x}$)	1	
Variační koeficient (V)	56 %	

Tabulka F.24: Nejhorší známka z ICT na vysvědčení, kterou respondenti dostali – otázka č. 7 (pouze 6. ročníky, n = 126).

Nejhorší známka z ICT	Četnost (n_i)	Relativní četnost (f_i)
1	100	62 %
2	29	18 %
3	25	15 %
4	6	4 %
5	1	1 %
Neměl(a) dosud ICT či obdobný předmět	1	1 %
Počet žáků, kteří již měli ICT či obdobný předmět	161	99 %
Aritmetický průměr ($\bar{x}$)	1,63	
Směrodatná odchylka (σ)	0,92	
Medián ($\tilde{x}$)	1	
Variační koeficient (V)	56 %	

Tabulka F.25: Nejhorší známka z ICT na vysvědčení, kterou respondenti dostali – otázka č. 7 (pouze 9. ročníky, n = 162).

Nejhorší známka z ICT	Četnost (n_i)	Relativní četnost (f_i)
1	53	60 %
2	12	14 %
3	2	2 %
4	2	2 %
5	0	0 %
Neměl(a) dosud ICT či obdobný předmět	19	22 %
Počet žáků, kteří již měli ICT či obdobný předmět	69	78 %
Aritmetický průměr ($\bar{x}$)	1,32	
Směrodatná odchylka (σ)	0,67	
Medián ($\tilde{x}$)	1	
Variační koeficient (V)	51 %	

Tabulka F.26: Nejhorší známka z ICT na vysvědčení, kterou respondenti dostali – otázka č. 7 (kontrolní skupina po výuce, n = 88).

Účty na sociálních sítích.	Četnost (n_i)	Relativní četnost (f_i)
Nemá účet na žádné sociální síti	38	13 %
Facebook	228	79 %
xTeen	21	7 %
Spolužáci	76	26 %
Twitter	30	10 %
Lidé.cz	54	19 %
MySpace	11	4 %
Google+	5	2 %
Badoo	7	2 %
Bebo	2	1 %
Youtube	7	2 %
Líbímseti	7	2 %

Tabulka F.27: Účty, které mají respondenti na jednotlivých sociálních sítích – otázka č. 8 (celý vzorek, n = 288).

Účty na sociálních sítích.	Četnost (n_i)	Relativní četnost (f_i)
Nemá účet na žádné sociální síti	25	20 %
Facebook	88	70 %
xTeen	11	9 %
Spolužáci	16	13 %
Twitter	14	11 %
Lidé.cz	21	17 %
MySpace	1	1 %
Google+	2	2 %
Badoo	1	1 %
Bebo	0	0 %
Youtube	4	3 %
Líbímseti	1	1 %

Tabulka F.28: Účty, které mají respondenti na jednotlivých sociálních sítích – otázka č. 8 (pouze 6. ročníky, n = 126).

Účty na sociálních sítích.	Četnost (n_i)	Relativní četnost (f_i)
Nemá účet na žádné sociální síti	13	8 %
Facebook	140	86 %
xTeen	10	6 %
Spolužáci	60	37 %
Twitter	16	10 %
Lidé.cz	33	20 %
MySpace	10	6 %
Google+	3	2 %
Badoo	6	4 %
Bebo	2	1 %
Youtube	3	2 %
Líbímseti	6	4 %

Tabulka F.29: Účty, které mají respondenti na jednotlivých sociálních sítích – otázka č. 8 (pouze 9. ročníky, n = 162).

Účty na sociálních sítích.	Četnost (n_i)	Relativní četnost (f_i)
Nemá účet na žádné sociální síti	14	16 %
Facebook	66	75 %
xTeen	7	8 %
Spolužáci	10	11 %
Twitter	8	9 %
Lidé.cz	16	18 %
MySpace	2	2 %
Google+	0	0 %
Badoo	0	0 %
Bebo	0	0 %
Youtube	0	0 %
Líbímseti	0	0 %

Tabulka F.30: Účty, které mají respondenti na jednotlivých sociálních sítích – otázka č. 8 (kontrolní skupina po výuce, n = 88).

Četli podmínky?	Četnost (n_i)	Relativní četnost (f_i)
Ano	104	42 %
Začal(a) číst, ale nedočetl(a)	79	32 %
Ne	67	27 %

Tabulka F.31: Četli respondenti podmínky sociálních sítí, na kterých mají účet? – otázka č. 9 (celý vzorek, n = 250).

Četli podmínky?	Četnost (n_i)	Relativní četnost (f_i)
Ano	57	56 %
Začal(a) číst, ale nedočetl(a)	24	24 %
Ne	20	20 %

Tabulka F.32: Četli respondenti podmínky sociálních sítí, na kterých mají účet? – otázka č. 9 (pouze 6. ročníky, n = 101).

Četli podmínky?	Četnost (n_i)	Relativní četnost (f_i)
Ano	47	32 %
Začal(a) číst, ale nedočetl(a)	55	37 %
Ne	47	32 %

Tabulka F.33: Četli respondenti podmínky sociálních sítí, na kterých mají účet? – otázka č. 9 (pouze 9. ročníky, n = 148).

Četli podmínky?	Četnost (n_i)	Relativní četnost (f_i)
Ano	10	14 %
Začal(a) číst, ale nedočetl(a)	29	39 %
Ne	35	47 %

Tabulka F.34: Četli respondenti podmínky sociálních sítí, na kterých mají účet? – otázka č. 9 (kontrolní skupina po výuce, n = 74).

Vědí o nastavení soukromí na Facebooku?	Četnost (n_i)	Relativní četnost (f_i)
Ano	214	94 %
Ne	14	6 %

Tabulka F.35: Vědí respondenti, kteří mají účet na Facebooku, o možnostech nastavení soukromí? – otázka č. 10 (celý vzorek, n = 228).

Vědí o nastavení soukromí na Facebooku?	Četnost (n_i)	Relativní četnost (f_i)
Ano	79	90 %
Ne	9	10 %

Tabulka F.36: Vědí respondenti, kteří mají účet na Facebooku, o možnostech nastavení soukromí? – otázka č. 10 (pouze 6. ročníky, n = 88).

Vědí o nastavení soukromí na Facebooku?	Četnost (n_i)	Relativní četnost (f_i)
Ano	135	96 %
Ne	5	4 %

Tabulka F.37: Vědí respondenti, kteří mají účet na Facebooku, o možnostech nastavení soukromí? – otázka č. 10 (pouze 9. ročníky, n = 140).

Vědí o nastavení soukromí na Facebooku?	Četnost (n_i)	Relativní četnost (f_i)
Ano	65	98 %
Ne	1	2 %

Tabulka F.38 Vědí respondenti, kteří mají účet na Facebooku, o možnostech nastavení soukromí? – otázka č. 10 (kontrolní skupina po výuce, n = 66).

Využívají nastavení soukromí na Facebooku?	Četnost (n_i)	Relativní četnost (f_i)
Ano	188	82 %
Ne	40	18 %

Tabulka F.39: Využívají respondenti, kteří mají účet na Facebooku, možnosti nastavení soukromí? – otázka č. 11 (celý vzorek, n = 228).

Využívají nastavení soukromí na Facebooku?	Četnost (n_i)	Relativní četnost (f_i)
Ano	72	82 %
Ne	16	18 %

Tabulka F.40: Využívají respondenti, kteří mají účet na Facebooku, možnosti nastavení soukromí? – otázka č. 11 (pouze 6. ročníky, n = 88).

Využívají nastavení soukromí na Facebooku?	Četnost (n_i)	Relativní četnost (f_i)
Ano	116	83 %
Ne	24	17 %

Tabulka F.41: Využívají respondenti, kteří mají účet na Facebooku, možnosti nastavení soukromí? – otázka č. 11 (pouze 9. ročníky, n = 140).

Využívají nastavení soukromí na Facebooku?	Četnost (n_i)	Relativní četnost (f_i)
Ano	61	92 %
Ne	5	8 %

Tabulka F.42: Využívají respondenti, kteří mají účet na Facebooku, možnosti nastavení soukromí? – otázka č. 11 (kontrolní skupina po výuce, n = 66).

S kým se přátelí na Facebooku?	Četnost (n_i)	Relativní četnost (f_i)
Přátelím se s lidmi, které vídám, ale neznáme se osobně	119	52 %
Přátelím se s přáteli přátel, i když je jinak neznám.	35	15 %
Přátelím se s kýmkoliv, kdo mi pošle nabídku k přátelství a nevypadá podezřele.	12	5 %
Přátelím se s kýmkoliv, kdo má podobný zájem vyplněný v profilu	12	5 %
Přátelím se s kýmkoliv, kdo mi pošle nabídku k přátelství a je to můj vrstevník.	9	4 %
Přátelím se s kýmkoliv, kdo mi pošle nabídku k přátelství.	8	4 %

Tabulka F.43: S kým se respondenti přátelí na Facebooku? – otázka č. 12 (celý vzorek, n = 228).

S kým se přátelí na Facebooku?	Četnost (n_i)	Relativní četnost (f_i)
Přátelím se s lidmi, které vídám, ale neznáme se osobně	27	31 %
Přátelím se s přáteli přátel, i když je jinak neznám.	9	10 %
Přátelím se s kýmkoliv, kdo mi pošle nabídku k přátelství a nevypadá podezřele.	4	5 %
Přátelím se s kýmkoliv, kdo má podobný zájem vyplněný v profilu	7	8 %
Přátelím se s kýmkoliv, kdo mi pošle nabídku k přátelství a je to můj vrstevník.	4	5 %
Přátelím se s kýmkoliv, kdo mi pošle nabídku k přátelství.	4	5 %

Tabulka F.44: S kým se respondenti přátelí na Facebooku? – otázka č. 12 (pouze 6. ročníky, n = 88).

S kým se přátelí na Facebooku?	Četnost (n_i)	Relativní četnost (f_i)
Přátelím se s lidmi, které vídám, ale neznáme se osobně	92	66 %
Přátelím se s přáteli přátel, i když je jinak neznám.	26	19 %
Přátelím se s kýmkoliv, kdo mi pošle nabídku k přátelství a nevypadá podezřele.	8	6 %
Přátelím se s kýmkoliv, kdo má podobný zájem vyplněný v profilu	5	4 %
Přátelím se s kýmkoliv, kdo mi pošle nabídku k přátelství a je to můj vrstevník.	5	4 %
Přátelím se s kýmkoliv, kdo mi pošle nabídku k přátelství.	4	3 %

Tabulka F.45: S kým se respondenti přátelí na Facebooku? – otázka č. 12 (pouze 9. ročníky, n = 140).

S kým se přátelí na Facebooku?	Četnost (n_i)	Relativní četnost (f_i)
Přátelím se s lidmi, které vídám, ale neznáme se osobně	31	47%
Přátelím se s přáteli přátel, i když je jinak neznám.	1	2%
Přátelím se s kýmkoliv, kdo mi pošle nabídku k přátelství a nevypadá podezřele.	3	5%
Přátelím se s kýmkoliv, kdo má podobný zájem vyplněný v profilu	2	3%
Přátelím se s kýmkoliv, kdo mi pošle nabídku k přátelství a je to můj vrstevník.	1	2%
Přátelím se s kýmkoliv, kdo mi pošle nabídku k přátelství.	2	3%

Tabulka F.46: S kým se respondenti přátelí na Facebooku? – otázka č. 12 (kontrolní skupina po výuce, n = 66).

Údaje zveřejňované na internetu	Četnost (n_i)	Relativní četnost (f_i)
Jméno	254	88 %
Příjmení	234	81 %
Rok narození (věk)	149	52 %
Datum narození (narozeniny)	171	59 %
Město (bydliště)	116	40 %
Fotografie obličeje	159	55 %
Karikaturu	14	5 %
Škola	89	31 %
E-mailová adresa	166	58 %
Kontaktní údaje (ICQ, Skype...)	32	11 %
Telefon	16	6 %
Adresa	13	5 %
Rodné číslo	5	2 %
Žádný z údajů	23	8 %
Celé datum narození	125	43 %
Adresa doplněná o jméno a příjmení	13	5 %
Aritmetický průměr počtu zveřej. údajů ($\bar{x}$)	4,92	
Směrodatná odchylka počtu zveřej. údajů (σ)	2,56	
Medián počtu zveřej. údajů ($\tilde{x}$)	5	
Variační koeficient počtu zveřej. údajů (V)	52%	

Tabulka F.47: Údaje, které o sobě respondenti zveřejňují na internetu. – otázka č. 13 (celý vzorek, n = 288).

Údaje zveřejňované na internetu	Četnost (n_i)	Relativní četnost (f_i)
Jméno	103	82 %
Příjmení	92	73 %
Rok narození (věk)	57	45 %
Datum narození (narozeniny)	61	48 %
Město (bydliště)	42	33 %
Fotografie obličeje	55	44 %
Karikaturu	4	3 %
Škola	40	32 %
E-mailová adresa	68	54 %
Kontaktní údaje (ICQ, Skype...)	15	12 %
Telefon	7	6 %
Adresa	7	6 %
Rodné číslo	1	1 %
Žádný z údajů	19	15 %
Celé datum narození	45	36 %
Adresa doplněná o jméno a příjmení	7	6 %
Aritmetický průměr počtu zveřej. údajů ($\bar{x}$)	4,38	
Směrodatná odchylka počtu zveřej. údajů (σ)	2,73	
Medián počtu zveřej. údajů ($\tilde{x}$)	4	
Variační koeficient počtu zveřej. údajů (V)	62 %	

Tabulka F.48: Údaje, které o sobě respondenti zveřejňují na internetu. – otázka č. 13 (pouze 6. ročníky, n = 126).

Údaje zveřejňované na internetu	Četnost (n_i)	Relativní četnost (f_i)
Jméno	151	93 %
Příjmení	142	88 %
Rok narození (věk)	92	57 %
Datum narození (narozeniny)	110	68 %
Město (bydliště)	74	46 %
Fotografie obličeje	104	64 %
Karikaturu	10	6 %
Škola	49	30 %
E-mailová adresa	98	60 %
Kontaktní údaje (ICQ, Skype...)	17	10 %
Telefon	9	6 %
Adresa	6	4 %
Rodné číslo	4	2 %
Žádný z údajů	4	2 %
Celé datum narození	80	49 %
Adresa doplněná o jméno a příjmení	6	4 %
Aritmetický průměr počtu zveřej. údajů ($\bar{x}$)	5,35	
Směrodatná odchylka počtu zveřej. údajů (σ)	2,34	
Medián počtu zveřej. údajů ($\tilde{x}$)	6	
Variační koeficient počtu zveřej. údajů (V)	44 %	

Tabulka F.49: Údaje, které o sobě respondenti zveřejňují na internetu. – otázka č. 13 (pouze 9. ročníky, n = 162).

Údaje zveřejňované na internetu	Četnost (n_i)	Relativní četnost (f_i)
Jméno	76	86 %
Příjmení	62	70 %
Rok narození (věk)	40	45 %
Datum narození (narozeniny)	46	52 %
Město (bydliště)	31	35 %
Fotografie obličeje	37	42 %
Karikaturu	6	7 %
Škola	22	25 %
E-mailová adresa	47	53 %
Kontaktní údaje (ICQ, Skype...)	4	5 %
Telefon	3	3 %
Adresa	0	0 %
Rodné číslo	0	0 %
Žádný z údajů	6	7 %
Celé datum narození	32	36 %
Adresa doplněná o jméno a příjmení	0	0 %
Aritmetický průměr počtu zveřej. údajů ($\bar{x}$)	4,25	
Směrodatná odchylka počtu zveřej. údajů (σ)	2,34	
Medián počtu zveřej. údajů ($\tilde{x}$)	4	
Variační koeficient počtu zveřej. údajů (V)	55 %	

Tabulka F.50: Údaje, které o sobě respondenti zveřejňují na internetu. – otázka č. 13 (kontrol. sk. po výuce, n = 88).

Bodové hodnocení rizika zveřej-ňovaných údajů	Četnost (n_i)	Relativní četnost (f_i)
0 b.	123	43 %
1 b.	139	48 %
2 b.	15	5 %
3 b.	6	2 %
4 b.	3	1 %
5 b.	0	0 %
6 b.	2	1 %
Aritmetický průměr ($\bar{x}$)	0,73 b.	
Směrodatná odchylka (σ)	0,87 b.	
Medián ($\tilde{x}$)	1 b.	
Variační koeficient (V)	119 %	

Tabulka F.51: Bodové hodnocení zveřejňovaných údajů (ot. č. 13) (celý vzorek, n = 288).

Bodové hodnocení rizika zveřej-ňovaných údajů	Četnost (n_i)	Relativní četnost (f_i)
0 b.	64	51 %
1 b.	50	40 %
2 b.	8	6 %
3 b.	1	1 %
4 b.	3	2 %
Aritmetický průměr ($\bar{x}$)	0,64 b.	
Směrodatná odchylka (σ)	0,83 b.	
Medián ($\tilde{x}$)	0 b.	
Variační koeficient (V)	130 %	

Tabulka F.52: Bodové hodnocení zveřejňovaných údajů (ot. č. 13) (pouze 6. ročníky, n = 126).

Bodové hodnocení rizika zveřej-ňovaných údajů	Četnost (n_i)	Relativní četnost (f_i)
0 b.	59	36 %
1 b.	89	55 %
2 b.	7	4 %
3 b.	5	3 %
4 b.	0	0 %
5 b.	0	0 %
6 b.	2	1 %
Aritmetický průměr ($\bar{x}$)	0,80 b.	
Směrodatná odchylka (σ)	0,89 b.	
Medián ($\tilde{x}$)	1 b.	
Variační koeficient (V)	111 %	

Tabulka F.53: Bodové hodnocení zveřejňovaných údajů (ot. č. 13) (pouze 9. ročníky, n = 162).

Bodové hodnocení rizika zveřejňovaných údajů	Četnost (n_i)	Relativní četnost (f_i)
0 b.	49	56 %
1 b.	36	41 %
2 b.	3	3 %
Aritmetický průměr ($\bar{x}$)	0,48 b.	
Směrodatná odchylka (σ)	0,56 b.	
Medián ($\tilde{x}$)	1 b.	
Variační koeficient (V)	117 %	

Tabulka F.54: Bodové hodnocení zveřejňovaných údajů (ot. č. 13) (kontrolní skupina po výuce, n = 88).

Zveřejňování jakých údajů považují za nebezpečné?	Četnost (n_i)	Relativní četnost (f_i)
Jméno	46	16 %
Příjmení	65	23 %
Rok narození (věk)	73	25 %
Datum narození (narozeniny)	73	25 %
Město (bydliště)	112	39 %
Fotografie obličeje	44	15 %
Karikaturu	144	50 %
Škola	112	39 %
E-mailová adresa	92	32 %
Kontaktní údaje (ICQ, Skype...)	100	35 %
Telefon	225	78 %
Adresa	245	85 %
Rodné číslo	225	78 %
Celé datum narození	46	16 %
Vše je bezpečné	24	8 %

Tabulka F.55: Zveřejňování kterých údajů považují respondenti za nebezpečné? – otázka č. 14 (celý vzorek, n = 288).

Zveřejňování jakých údajů považují za nebezpečné?	Četnost (n_i)	Relativní četnost (f_i)
Jméno	25	20 %
Příjmení	33	26 %
Rok narození (věk)	37	29 %
Datum narození (narozeniny)	39	31 %
Město (bydliště)	62	49 %
Fotografie obličeje	26	21 %
Karikaturu	65	52 %
Škola	50	40 %
E-mailová adresa	48	38 %
Kontaktní údaje (ICQ, Skype...)	66	52 %
Telefon	103	82 %
Adresa	104	83 %
Rodné číslo	94	75 %
Celé datum narození	23	18 %
Vše je bezpečné	4	3 %

Tabulka F.56: Zveřejňování kterých údajů považují respondenti za nebezpečné? – otázka č. 14 (pouze 6. ročníky, n = 126).

Zveřejňování jakých údajů považují za nebezpečné?	Četnost (n_i)	Relativní četnost (f_i)
Jméno	21	13 %
Příjmení	32	20 %
Rok narození (věk)	36	22 %
Datum narození (narozeniny)	34	21 %
Město (bydliště)	50	31 %
Fotografie obličeje	18	11 %
Karikaturu	79	49 %
Škola	62	38 %
E-mailová adresa	44	27 %
Kontaktní údaje (ICQ, Skype...)	34	21 %
Telefon	122	75 %
Adresa	141	87 %
Rodné číslo	131	81 %
Celé datum narození	23	14 %
Vše je bezpečné	20	12 %

Tabulka F.57: Zveřejňování kterých údajů považují respondenti za nebezpečné? – otázka č. 14 (pouze 9. ročníky, n = 162).

Zveřejňování jakých údajů považují za nebezpečné?	Četnost (n_i)	Relativní četnost (f_i)
Jméno	18	20%
Příjmení	33	38%
Rok narození (věk)	28	32%
Datum narození (narozeniny)	34	39%
Město (bydliště)	48	55%
Fotografie obličeje	13	15%
Karikaturu	48	55%
Škola	50	57%
E-mailová adresa	27	31%
Kontaktní údaje (ICQ, Skype...)	38	43%
Telefon	69	78%
Adresa	72	82%
Rodné číslo	74	84%
Celé datum narození	17	19%
Vše je bezpečné	3	3%

Tabulka F.58: Zveřejňování kterých údajů považují respondenti za nebezpečné? – Otázka č. 14 (kontrolní skupina po výuce, n = 88).

Půjčili někdy někomu svůj účet?	Četnost (n_i)	Relativní četnost (f_i)
Ano	72,00	25 %
Ne	216,00	75 %

Tabulka F.59: Půjčili respondenti někdy někomu svůj elektronický účet? – Otázka č. 15 (celý vzorek, n = 288).

Půjčili někdy někomu svůj účet?	Četnost (n_i)	Relativní četnost (f_i)
Ano	27,00	21 %
Ne	99,00	79 %

Tabulka F.60: Půjčili respondenti někdy někomu svůj elektronický účet? – Otázka č. 15 (pouze 6. ročníky, n = 126).

Půjčili někdy někomu svůj účet?	Četnost (n_i)	Relativní četnost (f_i)
Ano	45	28 %
Ne	117	72 %

Tabulka F.61: : Půjčili respondenti někdy někomu svůj elektronický účet? – Otázka č. 15 (pouze 9. ročníky, n = 162).

Půjčili někdy někomu svůj účet?	Četnost (n_i)	Relativní četnost (f_i)
Ano	17	19 %
Ne	71	81 %

Tabulka F.62: Půjčili respondenti někdy někomu svůj elektronický účet? – Otázka č. 15 (kontrolní skupina po výuce, n = 88).

Prolomili jejich účet?	Četnost (n_i)	Relativní četnost (f_i)
Ano	51	18 %
Ne	237	82 %

Tabulka F.63: Prolomili již někdy respondentům elektronický účet? – otázka č. 16 (celý vzorek, n = 288).

Prolomili jejich účet?	Četnost (n_i)	Relativní četnost (f_i)
Ano	25	20 %
Ne	101	80 %

Tabulka F.64: Prolomili již někdy respondentům elektronický účet? – otázka č. 16 (pouze 6. ročníky, n = 126).

Prolomili jejich účet?	Četnost (n_i)	Relativní četnost (f_i)
Ano	26	16 %
Ne	136	84 %

Tabulka F.65: Prolomili již někdy respondentům elektronický účet? – otázka č. 16 (pouze 9. ročníky, n = 162).

Prolomili jejich účet?	Četnost (n_i)	Relativní četnost (f_i)
Ano	13	15 %
Ne	75	85 %

Tabulka F.66: Prolomili již někdy respondentům elektronický účet? – otázka č. 16 (kontrolní skupina po výuce, n = 88).

Myslí, že používají bezpečné heslo?	Četnost (n_i)	Relativní četnost (f_i)
Ano	264	92 %
Ne	24	8 %

Tabulka F.67: Myslí si respondenti, že používají bezpečné heslo – otázka č. 17 (celý vzorek, n = 288).

Myslí, že používají bezpečné heslo?	Četnost (n_i)	Relativní četnost (f_i)
Ano	113	90 %
Ne	13	10 %

Tabulka F.68: Myslí si respondenti, že používají bezpečné heslo – otázka č. 17 (pouze 6. ročníky, n = 126).

Myslí, že používají bezpečné heslo?	Četnost (n_i)	Relativní četnost (f_i)
Ano	151	93 %
Ne	11	7 %

Tabulka F.69: Myslí si respondenti, že používají bezpečné heslo – otázka č. 17 (pouze 9. ročníky, n = 162).

Myslí, že používají bezpečné heslo?	Četnost (n_i)	Relativní četnost (f_i)
Ano	79	90 %
Ne	9	10 %

Tabulka F.70: : Myslí si respondenti, že používají bezpečné heslo – otázka č. 17 (kontrolní skupina po výuce, n = 88).

Používají pro každý elektronický účet jiné heslo?	Četnost (n_i)	Relativní četnost (f_i)
Ne, používám všude stejné heslo.	46	16 %
Ne, ale používám více hesel.	124	43 %
Ano	118	41 %

Tabulka F.71: Používají respondenti pro každý účet jiné heslo? – otázka č. 18 (celý vzorek, n = 288).

Používají pro každý elektronický účet jiné heslo?	Četnost (n_i)	Relativní četnost (f_i)
Ne, používám všude stejné heslo.	19	15 %
Ne, ale používám více hesel.	46	37 %
Ano	61	48 %

Tabulka F.72: : Používají respondenti pro každý účet jiné heslo? – otázka č. 18 (pouze 6. ročníky, n = 126).

Používají pro každý elektronický účet jiné heslo?	Četnost (n_i)	Relativní četnost (f_i)
Ne, používám všude stejné heslo.	27	17 %
Ne, ale používám více hesel.	78	48 %
Ano	57	35 %

Tabulka F.73: Používají respondenti pro každý účet jiné heslo? – otázka č. 18 (pouze 9. ročníky, n = 162).

Používají pro každý elektronický účet jiné heslo?	Četnost (n_i)	Relativní četnost (f_i)
Ne, používám všude stejné heslo.	3	3 %
Ne, ale používám více hesel.	36	41 %
Ano	49	56 %

Tabulka F.74: Používají respondenti pro každý účet jiné heslo? – otázka č. 18 (kontrolní skupina po výuce, n = 88).

Používají nějaký nástroj na ověření síly hesla?	Četnost (n_i)	Relativní četnost (f_i)
Ano	79	27 %
Ne	209	73 %

Tabulka F.75: Používají respondenti nějaký nástroj na ověření síly hesla? – otázka č. 19 (celý vzorek, n = 288).

Používají nějaký nástroj na ověření síly hesla?	Četnost (n_i)	Relativní četnost (f_i)
Ano	42	33%
Ne	84	67%

Tabulka F.76: Používají respondenti nějaký nástroj na ověření síly hesla? – otázka č. 19 (pouze 6. ročníky, n = 126).

Používají nějaký nástroj na ověření síly hesla?	Četnost (n_i)	Relativní četnost (f_i)
Ano	37	23 %
Ne	125	77 %

Tabulka F.77: Používají respondenti nějaký nástroj na ověření síly hesla? – otázka č. 19 (pouze 9. ročníky, n = 162).

Používají nějaký nástroj na ověření síly hesla?	Četnost (n_i)	Relativní četnost (f_i)
Ano	38	43 %
Ne	50	57 %

Tabulka F.78: Používají respondenti nějaký nástroj na ověření síly hesla? – otázka č. 19 (kontrolní skupina po výuce, n = 88).

Znají nějaké programy pro správu hesel?	Četnost (n_i)	Relativní četnost (f_i)
Ano	64	22 %
Ne	224	78 %

Tabulka F.79: Znají respondenti nějaké nástroje pro správu hesel? – otázka č. 20 (celý vzorek, n = 288).

Znají nějaké programy pro správu hesel?	Četnost (n_i)	Relativní četnost (f_i)
Ano	28	22 %
Ne	98	78 %

Tabulka F.80: Znají respondenti nějaké nástroje pro správu hesel? – otázka č. 20 (pouze 6. ročníky, n = 126).

Znají nějaké programy pro správu hesel?	Četnost (n_i)	Relativní četnost (f_i)
Ano	36	22 %
Ne	126	78 %

Tabulka F.81: Znají respondenti nějaké nástroje pro správu hesel? – otázka č. 20 (pouze 9. ročníky, n = 162).

Znají nějaké programy pro správu hesel?	Četnost (n_i)	Relativní četnost (f_i)
Ano	45	51 %
Ne	43	49 %

Tabulka F.82: Znají respondenti nějaké nástroje pro správu hesel? – otázka č. 20 (kontrolní skupina po výuce, n = 88).

Používají správce hesel?	Četnost (n_i)	Relativní četnost (f_i)
Ano	39	14 %
Ne	249	86 %

Tabulka F.83:Používají respondenti nějaké nástroje pro správu hesel? – otázka č. 21 (celý vzorek, n = 288).

Používají správce hesel?	Četnost (n_i)	Relativní četnost (f_i)
Ano	18	14 %
Ne	108	86 %

Tabulka F.84:Používají respondenti nějaké nástroje pro správu hesel? – otázka č. 21 (pouze 6. ročníky, n = 126).

Používají správce hesel?	Četnost (n_i)	Relativní četnost (f_i)
Ano	21	13 %
Ne	141	87 %

Tabulka F.85: Používají respondenti nějaké nástroje pro správu hesel? – otázka č. 21 (pouze 9. ročníky, n = 162).

Používají správce hesel?	Četnost (n_i)	Relativní četnost (f_i)
Ano	15	17 %
Ne	73	83 %

Tabulka F.86: Používají respondenti nějaké nástroje pro správu hesel? – otázka č. 21 (kontrolní skupina po výuce, n = 88).

Počet bodů	Četnost (n_i)	Relativní četnost (f_i)
0 b.	64	22 %
1 b.	89	31 %
2 b.	92	32 %
3 b.	39	14 %
4 b.	4	1 %
Aritmetický průměr ($\bar{x}$)	1,41 b.	
Směrodatná odchylka (σ)	1,02 b.	
Medián ($\tilde{x}$)	1 b.	
Variační koeficient (V)	72 %	

Tabulka F.87: Bodové hodnocení kvality nejpoužívanějšího hesla – otázka č. 22 (celý vzorek n = 288).

Počet bodů	Četnost (n_i)	Relativní četnost (f_i)
0 b.	25	20 %
1 b.	44	35 %
2 b.	37	29 %
3 b.	18	14 %
4 b.	2	2 %
Aritmetický průměr ($\bar{x}$)	1,43 b.	
Směrodatná odchylka (σ)	1,01 b.	
Medián ($\tilde{x}$)	1 b.	
Variační koeficient (V)	71 %	

Tabulka F.88: Bodové hodnocení kvality nejpoužívanějšího hesla – otázka č. 22 (pouze 6. ročníky, n = 126).

Počet bodů	Četnost (n_i)	Relativní četnost (f_i)
0 b.	39	24 %
1 b.	45	28 %
2 b.	55	34 %
3 b.	21	13 %
4 b.	2	1 %
Aritmetický průměr ($\bar{x}$)	1,40 b.	
Směrodatná odchylka (σ)	1,03 b.	
Medián ($\tilde{x}$)	1 b.	
Variační koeficient (V)	74 %	

Tabulka F.89: Bodové hodnocení kvality nejpoužívanějšího hesla – otázka č. 22 (pouze 9. ročníky, n = 162).

Počet bodů	Četnost (n_i)	Relativní četnost (f_i)
0 b.	36	41 %
1 b.	26	30 %
2 b.	19	22 %
3 b.	7	8 %
Aritmetický průměr ($\bar{x}$)	0,97 b.	
Směrodatná odchylka (σ)	0,97 b.	
Medián ($\tilde{x}$)	1 b.	
Variační koeficient (V)	100 %	

Tabulka F.90: Bodové hodnocení kvality nejpoužívanějšího hesla – otázka č. 22 (kontrolní skupina po výuce, n = 88).

Návyky spojené s nejpoužívanějším heslem.	Četnost (n_i)	Relativní četnost (f_i)
Heslo sděluje rodičům (0 b.)	58	20 %
Heslo sděluje nejlepšímu kamarádovi (kamarádce) (1 b.)	33	11 %
Heslo sděluje někomu dalšímu (1 b.)	3	1 %
Heslo má uložené v nezaheslovaném souboru (1 b.)	2	1 %
Heslo má zapsané na lístečku a vystavené u počítače (1 b.)	5	2 %
Heslo má zapsané na lístečku a schované (0 b.)	27	9 %
Heslo má uložené na jiném médiu (0 b.)	9	3 %
Heslo má uložené v manažeru hesel (0 b.)	7	2 %

Tabulka F.91: Návyky respondentů spojené s nejpoužívanějším heslem. – otázka č. 23 (celý vzorek n = 288).

Návyky spojené s nejpoužívanějším heslem.	Četnost (n_i)	Relativní četnost (f_i)
Heslo sděluje rodičům (0 b.)	40	32 %
Heslo sděluje nejlepšímu kamarádovi (kamarádce) (1 b.)	11	9 %
Heslo sděluje někomu dalšímu (1 b.)	0	0 %
Heslo má uložené v nezaheslovaném souboru (1 b.)	0	0 %
Heslo má zapsané na lístečku a vystavené u počítače (1 b.)	3	2 %
Heslo má zapsané na lístečku a schované (0 b.)	12	10 %
Heslo má uložené na jiném médiu (0 b.)	4	3%
Heslo má uložené v manažeru hesel (0 b.)	3	2%

Tabulka F.92: Návyky respondentů spojené s nejpoužívanějším heslem. – otázka č. 23 (pouze 6. ročníky, n = 126).

Návyky spojené s nejpoužívanějším heslem.	Četnost (n_i)	Relativní četnost (f_i)
Heslo sděluje rodičům (0 b.)	18	11 %
Heslo sděluje nejlepšímu kamarádovi (kamarádce) (1 b.)	22	14 %
Heslo sděluje někomu dalšímu (1 b.)	3	2 %
Heslo má uložené v nezaheslovaném souboru (1 b.)	2	1 %
Heslo má zapsané na lístečku a vystavené u počítače (1 b.)	2	1 %
Heslo má zapsané na lístečku a schované (0 b.)	15	9 %
Heslo má uložené na jiném médiu (0 b.)	5	3 %
Heslo má uložené v manažeru hesel (0 b.)	4	2 %

Tabulka F.93: Návyky respondentů spojené s nejpoužívanějším heslem. – otázka č. 23 (pouze 9. ročníky, n = 162).

Návyky spojené s nejpoužívanějším heslem.	Četnost (n_i)	Relativní četnost (f_i)
Heslo sděluje rodičům (0 b.)	16	18 %
Heslo sděluje nejlepšímu kamarádovi (kamarádce) (1 b.)	5	6 %
Heslo sděluje někomu dalšímu (1 b.)	0	0 %
Heslo má uložené v nezaheslovaném souboru (1 b.)	0	0 %
Heslo má zapsané na lístečku a vystavené u počítače (1 b.)	1	1 %
Heslo má zapsané na lístečku a schované (0 b.)	7	8 %
Heslo má uložené na jiném médiu (0 b.)	1	1 %
Heslo má uložené v manažeru hesel (0 b.)	1	1 %

Tabulka F.94: Návyky respondentů spojené s nejpoužívanějším heslem. – otázka č. 23 (kontrolní skupina po výuce, n = 88).

Počet bodů	Četnost (n_i)	Relativní četnost (f_i)
0 b.	246	85 %
1 b.	41	14 %
2 b.	1	0 %

Tabulka F.95: Bodové hodnocení otázky č. 23 (celý vzorek n = 288).

Počet bodů	Četnost (n_i)	Relativní četnost (f_i)
0 b.	113	90 %
1 b.	12	10 %
2 b.	1	1 %

Tabulka F.96: Bodové hodnocení otázky č. 23 (pouze 6. ročníky, n = 126).

Počet bodů	Četnost (n_i)	Relativní četnost (f_i)
0 b.	133	82 %
1 b.	29	18 %
2 b.	0	0 %

Tabulka F.97: Bodové hodnocení otázky č. 23 (pouze 9. ročníky, n = 62).

Počet bodů	Četnost (n_i)	Relativní četnost (f_i)
0 b.	82	93 %
1 b.	6	7 %
2 b.	0	0 %

Tabulka F.98: Bodové hodnocení otázky č. 23 (kontrolní skupina po výuce, n = 88).

Vybrané heslo	Četnost (n_i)	Relativní četnost (f_i)
M!!p2o9 – 0 b.	233	81 %
Panacek5 – 1 b.	9	3 %
Vlak12 – 2 b.	3	1 %
hlgfn – 3 b.	26	9 %
motorka – 3 b.	5	2 %
12345678 – 4 b.	12	4 %
Aritmetický průměr ($\bar{x}$)	0,54 b.	
Směrodatná odchylka (σ)	1,19 b.	
Medián ($\tilde{x}$)	0 b.	
Variační koeficient (V)	220 %	

Tabulka F.99: Nejbezpečnější heslo z výběru dle respondentů – otázka č. 24 (celý vzorek n = 288).

Vybrané heslo	Četnost (n_i)	Relativní četnost (f_i)
M!!p2o9 – 0 b.	91	72 %
Panacek5 – 1 b.	4	3 %
Vlak12 – 2 b.	3	2 %
hlgfn – 3 b.	18	14 %
motorka – 3 b.	1	1 %
12345678 – 4 b.	9	7 %
Aritmetický průměr ($\bar{x}$)	0,82 b.	
Směrodatná odchylka (σ)	1,40 b.	
Medián ($\tilde{x}$)	0 b.	
Variační koeficient (V)	171 %	

Tabulka F.100: Nejbezpečnější heslo z výběru dle respondentů – otázka č. 24 (pouze 6. ročníky, n = 126).

Vybrané heslo	Četnost (n_i)	Relativní četnost (f_i)
M!!p2o9 – 0 b.	142	88 %
Panacek5 – 1 b.	5	3 %
Vlak12 – 2 b.	0	0 %
hlgfn – 3 b.	8	5 %
motorka – 3 b.	4	2 %
12345678 – 4 b.	3	2 %
Aritmetický průměr ($\bar{x}$)	0,33 b.	
Směrodatná odchylka (σ)	0,94 b.	
Medián ($\tilde{x}$)	0 b.	
Variační koeficient (V)	285 %	

Tabulka F.101: Nejbezpečnější heslo z výběru dle respondentů – otázka č. 24 (pouze 9. ročníky, n = 162).

Vybrané heslo	Četnost (n_i)	Relativní četnost (f_i)
M!!p2o9 – 0 b.	82	93 %
Panacek5 – 1 b.	2	2 %
Vlak12 – 2 b.	1	1 %
hlgfn – 3 b.	1	1 %
motorka – 3 b.	2	2 %
12345678 – 4 b.	0	0 %
Aritmetický průměr ($\bar{x}$)	0,15 b.	
Směrodatná odchylka (σ)	0,59 b.	
Medián ($\tilde{x}$)	0 b.	
Variační koeficient (V)	393 %	

Tabulka F.102: Nejbezpečnější heslo z výběru dle respondentů – otázka č. 24 (kontrolní skupina po výuce, n = 88).

Znají pojem HTTPS? (pochopení pojmu)	Četnost (n_i)	Relativní četnost (f_i)
Správná odpověď – 0 b.	121	42 %
Špatná odpověď – 1 b.	167	58 %

Tabulka F.103: Chápou respondenti význam pojmu HTTPS? Otázka č. 25 (celý vzorek n = 288).

Znají pojem HTTPS? (pochopení pojmu)	Četnost (n_i)	Relativní četnost (f_i)
Správná odpověď – 0 b.	48	38 %
Špatná odpověď – 1 b.	78	62 %

Tabulka F.104: Chápou respondenti význam pojmu HTTPS? Otázka č. 25 (pouze 6. ročníky, n = 126).

Znají pojem HTTPS? (pochopení pojmu)	Četnost (n_i)	Relativní četnost (f_i)
Správná odpověď – 0 b.	73	45 %
Špatná odpověď – 1 b.	89	55 %

Tabulka F.105: Chápou respondenti význam pojmu HTTPS? Otázka č. 25 (pouze 9. ročníky, n = 162).

Znají pojem HTTPS? (pochopení pojmu)	Četnost (n_i)	Relativní četnost (f_i)
Správná odpověď – 0 b.	71	81 %
Špatná odpověď – 1 b.	17	19 %

Tabulka F.106: Chápou respondenti význam pojmu HTTPS? Otázka č. 25 (kontrolní skupina po výuce, n = 88).

Reakce na phishingový mail.	Četnost (n_i)	Relativní četnost (f_i)
Poskytnutí osobních údajů - 2 b.	10	3 %
Telefonát na číslo uvedené v phishingové zprávě - 1 b.	25	9 %
Rozpoznání phishingové zprávy (neodpovídali) - 0 b.	253	88 %

Tabulka F.107: Reakce respondentů na phishingový mail – otázka č. 26 (celý vzorek n = 288).

Reakce na phishingový mail.	Četnost (n_i)	Relativní četnost (f_i)
Poskytnutí osobních údajů - 2 b.	5	4 %
Telefonát na číslo uvedené v phishingové zprávě - 1 b.	15	12 %
Rozpoznání phishingové zprávy (neodpovídali) - 0 b.	106	84 %

Tabulka F.108: Reakce respondentů na phishingový mail – otázka č. 26 (pouze 6. ročníky, n = 126).

Reakce na phishingový mail.	Četnost (n_i)	Relativní četnost (f_i)
Poskytnutí osobních údajů - 2 b.	5	3 %
Telefonát na číslo uvedené v phishingové zprávě - 1 b.	10	6 %
Rozpoznání phishingové zprávy (neodpovídali) - 0 b.	147	91 %

Tabulka F.109: Reakce respondentů na phishingový mail – otázka č. 26 (pouze 9. ročníky, n = 162).

Reakce na phishingový mail.	Četnost (n_i)	Relativní četnost (f_i)
Poskytnutí osobních údajů - 2 b.	0	0 %
Telefonát na číslo uvedené v phishingové zprávě - 1 b.	6	7 %
Rozpoznání phishingové zprávy (neodpovídali) - 0 b.	82	93 %

Tabulka F.110: Reakce respondentů na phishingový mail – otázka č. 26 (kontrolní skupina po výuce, n = 88).

Bodové hodnocení (ot. č. 13, 15, 16, 18, 22, 23, 24, 25, 26)	Četnost (n_i)	Relativní četnost (f_i)
0 b.	6	2 %
1 b.	19	7 %
2 b.	36	13 %
3 b.	39	14 %
4 b.	52	18 %
5 b.	36	13 %
6 b.	34	12 %
7 b.	25	9 %
8 b.	15	5 %
9 b.	10	3 %
10 b.	7	2 %
11 b.	3	1 %
12 b.	3	1 %
13 b.	2	1 %
14 b.	0	0 %
15 b.	0	0 %
16 b.	0	0 %
17 b.	1	0 %
1. kvartil (Q_1)	3 b.	
Medián ($\tilde{x}$)	4 b.	
3. kvartil (Q_3)	6 b.	
Aritmetický průměr ($\bar{x}$)	4,75 b.	
Směrodatná odchylka (σ)	2,70 b.	
Modus ($\hat{x}$)	4 b.	
Variační šíře (R)	17 b.	
Variační koeficient (V)	57 %	

Tabulka F.111: Bodové hodnocení otázek č. 13, 15, 16, 18, 22, 23, 24, 25, 26 (celý vzorek, n = 288).

Bodové hodnocení (ot. č. 13, 15, 16, 18, 22, 23, 24, 25, 26)	Četnost (n_i)	Relativní četnost (f_i)
0 b.	2	2 %
1 b.	8	6 %
2 b.	16	13 %
3 b.	18	14 %
4 b.	19	15 %
5 b.	16	13 %
6 b.	11	9 %
7 b.	15	12 %
8 b.	7	6 %
9 b.	7	6 %
10 b.	3	2 %
11 b.	1	1 %
12 b.	3	2 %
1. kvartil (Q_1)	3 b.	
Medián ($\tilde{x}$)	4,5 b.	
3. kvartil (Q_3)	7 b.	
Aritmetický průměr ($\bar{x}$)	4,90 b.	
Směrodatná odchylka (σ)	2,70 b.	
Modus ($\hat{x}$)	4 b.	
Variační šíře (R)	12 b.	
Variační koeficient (V)	55 %	

Tabulka F.112: Bodové hodnocení otázek č. 13, 15, 16, 18, 22, 23, 24, 25, 26 (pouze 6. ročníky, n = 126).

Bodové hodnocení (ot. č. 13, 15, 16, 18, 22, 23, 24, 25, 26)	Četnost (n_i)	Relativní četnost (f_i)
0 b.	4	2 %
1 b.	11	7 %
2 b.	20	12 %
3 b.	21	13 %
4 b.	33	20 %
5 b.	20	12 %
6 b.	23	14 %
7 b.	10	6 %
8 b.	8	5 %
9 b.	3	2 %
10 b.	4	2 %
11 b.	2	1 %
12 b.	0	0 %
13 b.	2	1 %
14 b.	0	0 %
15 b.	0	0 %
16 b.	0	0 %
17 b.	1	1 %
1. kvartil (Q_1)	3 b.	
Medián ($\tilde{x}$)	4 b.	
3. kvartil (Q_3)	6 b.	
Aritmetický průměr ($\bar{x}$)	4,63 b.	
Směrodatná odchylka (σ)	2,70 b.	
Modus ($\hat{x}$)	4 b.	
Variační šíře (R)	17 b.	
Variační koeficient (V)	58 %	

Tabulka F.113: Bodové hodnocení otázek č. 13, 15, 16, 18, 22, 23, 24, 25, 26 (pouze 9. ročníky, n = 162).

Bodové hodnocení (ot. č. 13, 15, 16, 18, 22, 23, 24, 25, 26)	Četnost (n_i)	Relativní četnost (f_i)
0 b.	4	3 %
1 b.	11	9 %
2 b.	17	14 %
3 b.	17	14 %
4 b.	26	22 %
5 b.	12	10 %
6 b.	15	13 %
7 b.	8	7 %
8 b.	5	4 %
9 b.	2	2 %
10 b.	2	2 %
11 b.	0	0 %
12 b.	1	1 %
1. kvartil (Q_1)	2 b.	
Medián ($\tilde{x}$)	4 b.	
3. kvartil (Q_3)	6 b.	
Aritmetický průměr ($\bar{x}$)	4,13 b.	
Směrodatná odchylka (σ)	2,34 b.	
Modus ($\hat{x}$)	4 b.	
Variační šíře (R)	12 b.	
Variační koeficient (V)	57 %	

Tabulka F.114: Bodové hodnocení otázek č. 13, 15, 16, 18, 22, 23, 24, 25, 26 (kontrolní skupina před výukou, n = 120).

Bodové hodnocení (ot. č. 13, 15, 16, 18, 22, 23, 24, 25, 26)	Četnost (n_i)	Relativní četnost (f_i)
0 b.	8	9 %
1 b.	21	24 %
2 b.	14	16 %
3 b.	14	16 %
4 b.	17	19 %
5 b.	9	10 %
6 b.	3	3 %
7 b.	0	0 %
8 b.	1	1 %
9 b.	0	0 %
10 b.	0	0 %
11 b.	1	1 %
1. kvartil (Q_1)	1 b.	
Medián ($\tilde{x}$)	3 b.	
3. kvartil (Q_3)	4 b.	
Aritmetický průměr ($\bar{x}$)	2,74 b.	
Směrodatná odchylka (σ)	1,95 b.	
Modus ($\hat{x}$)	1 b.	
Variační šíře (R)	11 b.	
Variační koeficient (V)	71 %	

Tabulka F.115: Bodové hodnocení otázek č. 13, 15, 16, 18, 22, 23, 24, 25, 26 (kontrolní skupina po výuce, n = 88).

Bodové hodnocení (ot. č. 13, 18, 22, 23, 24, 25, 26).	Četnost (n_i)	Relativní četnost (f_i)
0 b.	8	3 %
1 b.	25	9 %
2 b.	38	13 %
3 b.	50	17 %
4 b.	49	17 %
5 b.	37	13 %
6 b.	28	10 %
7 b.	22	8 %
8 b.	13	5 %
9 b.	7	2 %
10 b.	5	2 %
11 b.	2	1 %
12 b.	3	1 %
13 b.	0	0 %
14 b.	0	0 %
15 b.	1	0 %
1. kvartil (Q_1)	3 b.	
Medián ($\tilde{x}$)	4 b.	
3. kvartil (Q_3)	6 b.	
Aritmetický průměr ($\bar{x}$)	4,32 b.	
Směrodatná odchylka (σ)	2,53 b.	
Modus ($\hat{x}$)	4 b.	
Variační šíře (R)	15 b.	
Variační koeficient (V)	59 %	

Tabulka F.116: Bodové hodnocení otázek č. 13, 18, 22, 23, 24, 25, 26 (celý vzorek, n = 288).

Bodové hodnocení (ot. č. 13, 18, 22, 23, 24, 25, 26).	Četnost (n_i)	Relativní četnost (f_i)
0 b.	3	2 %
1 b.	11	9 %
2 b.	17	13 %
3 b.	19	15 %
4 b.	21	17 %
5 b.	17	13 %
6 b.	9	7 %
7 b.	14	11 %
8 b.	4	3 %
9 b.	5	4 %
10 b.	3	2 %
11 b.	1	1 %
12 b.	2	2 %
1. kvartil (Q_1)	3 b.	
Medián ($\tilde{x}$)	4 b.	
3. kvartil (Q_3)	6 b.	
Aritmetický průměr ($\bar{x}$)	4,48 b.	
Směrodatná odchylka (σ)	2,61 b.	
Modus ($\hat{x}$)	4 b.	
Variační šíře (R)	12 b.	
Variační koeficient (V)	58 %	

Tabulka F.117: Bodové hodnocení otázek č. 13, 18, 22, 23, 24, 25, 26 (pouze 6. ročníky, n = 126).

Bodové hodnocení (ot. č. 13, 18, 22, 23, 24, 25, 26).	Četnost (n_i)	Relativní četnost (f_i)
0 b.	5	3 %
1 b.	14	9 %
2 b.	21	13 %
3 b.	31	19 %
4 b.	28	17 %
5 b.	20	12 %
6 b.	19	12 %
7 b.	8	5 %
8 b.	9	6 %
9 b.	2	1 %
10 b.	2	1 %
11 b.	1	1 %
12 b.	1	1 %
13 b.	0	0 %
14 b.	0	0 %
15 b.	1	1 %
1. kvartil (Q_1)	3 b.	
Medián ($\tilde{x}$)	4 b.	
3. kvartil (Q_3)	6 b.	
Aritmetický průměr ($\bar{x}$)	4,19 b.	
Směrodatná odchylka (σ)	2,46 b.	
Modus ($\hat{x}$)	3 b.	
Variační šíře (R)	15 b.	
Variační koeficient (V)	59 %	

Tabulka F.118: Bodové hodnocení otázek č. 13, 18, 22, 23, 24, 25, 26 (pouze 9. ročníky, n = 162).

Bodové hodnocení (ot. č. 13, 18, 22, 23, 24, 25, 26).	Četnost (n_i)	Relativní četnost (f_i)
0 b.	6	5 %
1 b.	12	10 %
2 b.	17	14 %
3 b.	20	17 %
4 b.	27	23 %
5 b.	14	12 %
6 b.	10	8 %
7 b.	8	7 %
8 b.	3	3 %
9 b.	1	1 %
10 b.	2	2 %
1. kvartil (Q_1)	2 b.	
Medián ($\tilde{x}$)	4 b.	
3. kvartil (Q_3)	5 b.	
Aritmetický průměr ($\bar{x}$)	3,78 b.	
Směrodatná odchylka (σ)	2,15 b.	
Modus ($\hat{x}$)	4 b.	
Variační šíře (R)	10 b.	
Variační koeficient (V)	57 %	

Tabulka F.119: Bodové hodnocení otázek č. 13, 18, 22, 23, 24, 25, 26 Kontrolní skupina před výukou, n = 120).

Bodové hodnocení (ot. č. 13, 18, 22, 23, 24, 25, 26).	Četnost (n_i)	Relativní četnost (f_i)
0 b.	14	16 %
1 b.	16	18 %
2 b.	17	19 %
3 b.	21	24 %
4 b.	11	13 %
5 b.	5	6 %
6 b.	2	2 %
7 b.	0	0 %
8 b.	1	1 %
9 b.	1	1 %
1. kvartil (Q_1)	1 b.	
Medián ($\tilde{x}$)	2 b.	
3. kvartil (Q_3)	3 b.	
Aritmetický průměr ($\bar{x}$)	2,40 b.	
Směrodatná odchylka (σ)	1,80 b.	
Modus ($\hat{x}$)	3 b.	
Variační šíře (R)	9 b.	
Variační koeficient (V)	75 %	

Tabulka F.120: Bodové hodnocení otázek č. 13, 18, 22, 23, 24, 25, 26 (kontrolní skupina po výuce, n = 88).

Příloha G – Návrh nových aktivit

Čas (min)	Cíle, metoda, forma, fáze, obsah a popis aktivity	Poznámky, pomůcky
Až 10 min.	**Obsah:** Úvod do tématu – **„Nebezpečí na internetu“**. (Možno dále specifikovat na osobní údaje na internetu, záleží na pojetí hodiny) **Metoda:** Brainstorming. **Organizační forma:** Hromadná výuka. **Fáze:** Motivace. **Cíl:** Žák si uvědomí, že používáni internetu, může přinášet rizika (afektivní).	
Až 20 min.	**Obsah:** Představení vybraného manažeru hesel a popis jeho ovládání. (Může vhodně doplnit původní přednášku, kde jsou manažery a jejich funkce pouze zmíněny) **Metoda:** Instruktáž (slovní/názorně-demonstrační). **Organizační forma:** Frontální výuka. **Fáze:** Expozice. **Cíl:** Žák dokáže používat základní funkce vybraného manažeru hesel. (kognitivní)	
5 + 10 min.	**Obsah:** Představení vybrané sociální sítě žákem (žák průvodcem), diskuse o sociálních sítích, jejich výhodách, nevýhodách a rizicích (zde učitel vystupuje jako zdroj nápadů k hovoru, má v žácích vyvolávat pochybnosti, nadhazovat vhodná témata). **Organizační forma:** Hromadná výuka. **Metoda:** Inscenační (žák hraje přednášejícího na konferenci), zvolená metoda je na něm (Pravděpodobně slovní – výklad) + Slovní dialogická (následná debata) **Fáze:** Expozice + fixace. **Cíl:** Žák dokáže vyjmenovat, popsat a demonstrovat použití základních funkcí vybrané sociální. (kognitivní) Žák dokáže ocenit nabízené funkce a využije je při ochraně svého soukromí (afektivní)	Žák si může připravit podpůrnou prezentaci, obrázky, vytvořit k tomuto účelu profil. Mimo jiné podporuje prezentační a argumentační schopnosti žáků.
DÚ (dle potřeb žáka) + 3 min./žák prezentace	**Obsah:** Žáci se pokusí najít ve svém e-mailu nebo v archivech phishingových zpráv vhodný příklad (domácí úkol) a na něm dokážou ostatním vysvětlit, co je na něm podezřelého. **Organizační forma:** Samostatná práce + frontální výuka (prezentace žákem). **Metoda:** Práce se službami na internetu (vyhledávač, e-mailový klient) + frontální výuka (prezentace žákem). **Fáze:** Fixace. **Cíl:** Žák dokáže analyzovat phishingový mail a odhalit jeho jednotlivé podezřelé složky. (kognitivní)	Možno seznámit žáky s archivem podvodných zpráv na HOAX.cz Mimo jiné podporuje prezentační a argumentační schopnosti žáků.